ZXR10 5900/5200 Series
All Gigabit-Port Intelligent Routing Switch
User Manual (Basic Configuration Volume)

Version 2.8.23.A

ZTE CORPORATION
ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park,
Nanshan District, Shenzhen,
P. R. China
518057
Tel: (86) 755 26771900
Fax: (86) 755 26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

Revision History

Revision No.	Revision Date	Revision Reason
R1.2	20091015	Edition update

Serial Number: sjzl20095126

About This Manual

Purpose

ZXR10 5900/5200 (V2.8.23.A) Series All Gigabit-Port Intelligent Routing Switch User Manual (Basic Configuration Volume) provides procedures and guidelines that support the operation on ZXR10 5900/5200 Series All Gigabit-Port Intelligent Routing Switch, including:

- ZXR10 5924 Gigabit Routing Switch
- ZXR10 5928 Gigabit Routing Switch
- ZXR10 5928–Fi Gigabit Routing Switch
- ZXR10 5952 Gigabit Routing Switch
- ZXR10 5224 Gigabit Convergence Switch
- ZXR10 5228 Gigabit Convergence Switch
- ZXR10 5228–FI Gigabit Convergence Switch
- ZXR10 5252 Gigabit Convergence Switch
- ZXR10 5928–PS Gigabit Convergence Switch

Intended Audience

This manual is intended for engineers and technicians who perform operation activities on ZXR10 5900/5200 All Gigabit-Port Intelligent Routing Switches.

Prerequisite Skill and Knowledge

To use the Basic Configuration Volume effectively, users should have a general understanding of OSI Model. Familiarity with the following is helpful,

- Protocols
- Routing concepts and Data Communication Terminologies

What Is in This Manual

The Basic Configuration Volume contains the following chapters:

TABLE 1 CHAPTER SUMMARY

Chapter	Summary
Chapter 1 Safety Description	This chapter describes the safety instructions and signs.
Chapter 2 Usage and Operation	This chapter describes ZXR10 5900/5200 configuration mode in common use.
Chapter 3 System Management	This chapter introduces file system management, file backup and restoration, software version upgrade.
Chapter 4 Interface Configuration	This chapter describes port parameters configuration , port mirroring function, loopback detection and DOM configuration.
Chapter 5 Network Protocol Configuration	This chapter describes IP address configuration and ARP configuration.

Chapter	Summary
Chapter 6 Switch Stack System	This chapter describes the content and related knowledge of stack system and related configuration.
Chapter 7 ACL Configuration	This chapter introduces ACL and related configuration.
Chapter 8 QoS Configuration	This chapter introduces QOS and related configuration.
Chapter 9 DHCP Configuration	This chapter introduces DHCP and related configuration.
Chapter 10 VRRP Configuration	This chapter introduces VRRP and related configuration.
Chapter 11 Network Management Configuration	This chapter introduces Network management configuration.
Chapter 12 DOT1X Configuration	This chapter introduces DOT1Xt configuration.
Chapter 13 Cluster Management Configuration	This chapter introduces Cluster Management configuration.
Chapter 14 IPTV Configuration	This chapter describes the content and related knowledge of IPTV and related configuration.
Chapter 15 VBAS Configuration	This chapter introduces VBAS configuration.
Chapter 16 ZESR Configuration	This chapter introduces ZESR configuration.
Chapter 17 Security Configuration	This chapter introduces Security configuration.
Chapter 18 POE Configuration	This chapter describes the content and related knowledge of POE and related configuration.

Related Documentation

The following documentation is related to this manual:

- ZXR10 5900/5200(V2.8.23.A) Series All Gigabit-Port Intelligent Routing Switch Hardware Manual
- ZXR10 5900/5200(V2.8.23.A) Series All Gigabit-Port Intelligent Routing Switch User Manual (Ethernet Switching Volume)
- ZXR10 5900/5200(V2.8.23.A) Series All Gigabit-Port Intelligent Routing Switch User Manual (Basic Configuration Volume)
- ZXR10 5900/5200(V2.8.23.A) Series All Gigabit-Port Intelligent Routing Switch User Manual (IPv4 Routing Volume)
- ZXR10 5900/5200(V2.8.23.A) Series All Gigabit-Port Intelligent Routing Switch User Manual (IPv6 Routing Volume)
- ZXR10 Router-Ethernet Switch Command Manual - Command Index

- ZXR10 Router-Ethernet Switch Command Manual - System Management
- ZXR10 Router-Ethernet Switch Command Manual - Functional System I
- ZXR10 Router-Ethernet Switch Command Manual - Functional System Volume II
- ZXR10 Router-Ethernet Switch Command Manual - Functional System Volume III
- ZXR10 Router/Ethernet Switch Command Manual — Functional System IV
- ZXR10 Router/Ethernet Switch Command Manual — Protocol Stack I
- ZXR10 Router/Ethernet Switch Command Manual — Protocol Stack II
- ZXR10 Router/Ethernet Switch Command Manual — Protocol Stack III
- ZXR10 Router/Ethernet Switch Information Manual

This page is intentionally blank.

Chapter 1

Safety Description

Table of Contents

Safety Introduction

Only qualified professionals are allowed to perform installation, operation and maintenance due to the high temperature and high voltage of the equipment.

Observe the local safety codes and relevant operation procedures during equipment installation, operation and maintenance to prevent personal injury or equipment damage. Safety precautions introduced in this manual are supplementary to the local safety codes.

ZTE bears no responsibility in case of universal safety operation requirements violation and safety standards violation in designing, manufacturing and equipment usage.

Symbol Descriptions

Contents deserving special attention during ZXR10 5900/5200 configuration are explained as follow.

Caution:

It indicates that the fault will happen if safety is ignored.

Note:

It provides additional information.

This page is intentionally blank.

Chapter 2

Usage and Operation

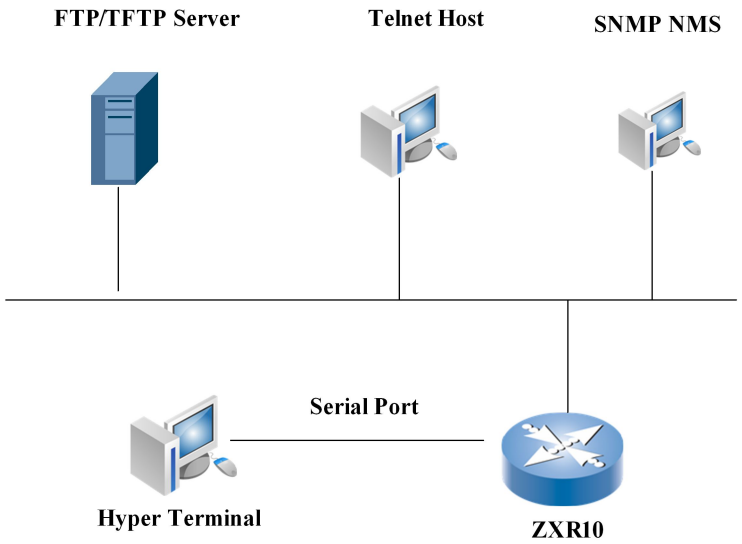
Table of Contents

Configuration Mode

As shown in Figure 1 , ZXR10 5900/5200 offers multiple configuration modes. A user can select configuration mode based on the connected network.

1. Configuration of Console Port Connection
2. TELNET Connection Configuration
3. SSH Secure Shell Connection Configuration
4. SNMP Connection Configuration

FIGURE 1 ZXR10 5900/5200 CONFIGURATION MODES



Configuring Through Console Port

This is main configuration mode of ZXR10 5900/5200. ZXR10 5900/5200 debugging configuration is implemented through the console port connection. The console port connection configuration adopts the VT100 terminal mode.

1. Select **Start > Programs > Accessories > Communications > HyperTerminal**on the PC screen to start the HyperTerminal, as shown in Figure 2 .

FIGURE 2 STARTING THE HYPERTERMINAL

2. Input the related local information in the interface as shown in Figure 3.

FIGURE 3 LOCATION INFORMATION

3. After the **Connection Description** dialog box appears, enter a name and choose an icon for the new connection, as shown in Figure 4.

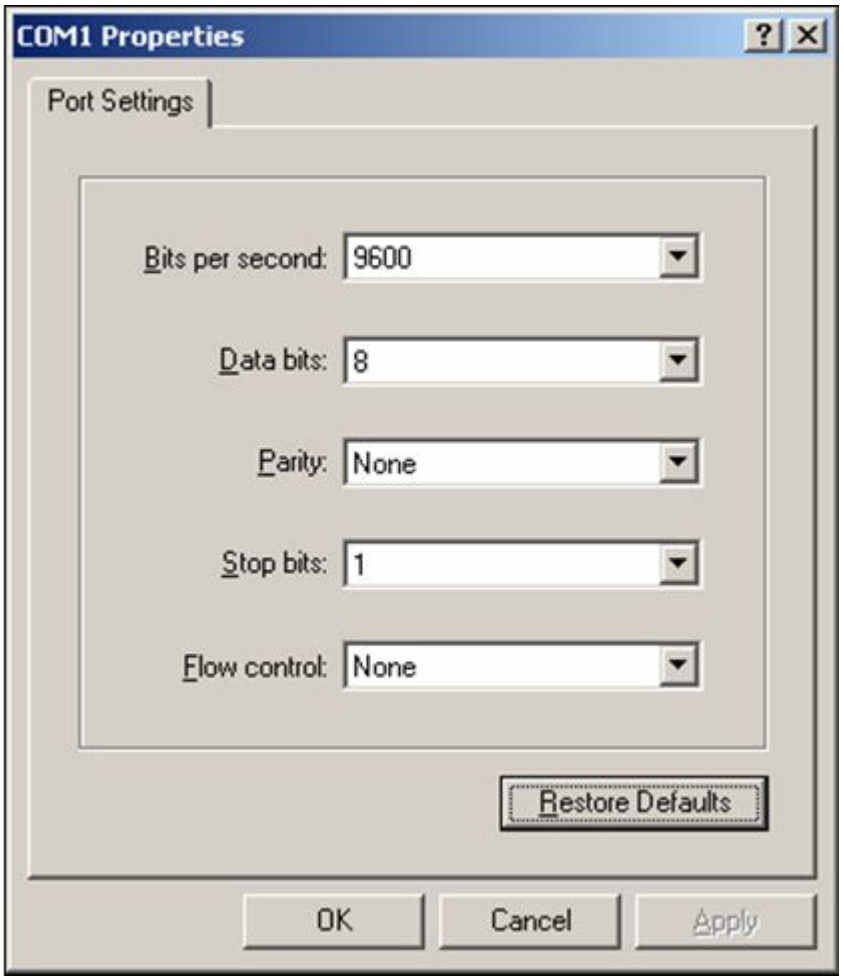
FIGURE 4 SETTING UP A CONNECTION

4. Based on serial port connection to the console cable, choose COM1 or COM2 as the serial port is to be connected, as shown in Figure 5 .

FIGURE 5 CONNECTION CONFIGURATION

5. Enter the properties of the selected serial port as shown in Figure 6 . The port property configuration includes: Bits per Second 9600, Data bit 8, Parity None, Stop bit 1, Data flow control None.

FIGURE 6 COM1 PROPERTIES



Power on and boot ZXR10 5900/5200 to initialize the system and to enter into configuration for operational use.

Telnet Connection Configuration

Telnet is the main remote configuration mode for the ZXR10 5900/5200.

Telnet access is set through user name and password. This enables unauthorized users from accessing the switch through Telnet. Use the following command to configure the user name and password.

username <*username*> **password** <*password*>

To strengthen the security of the switch, switch can limit telnet login of the users. Use the following command to admit or refuse telnet's IP address.

line telnet access-class <*basic access list*>

1. Connect the host directly to the switch and Telnet to the switch.

i. Configure the Telnet login user name and password through the console port.

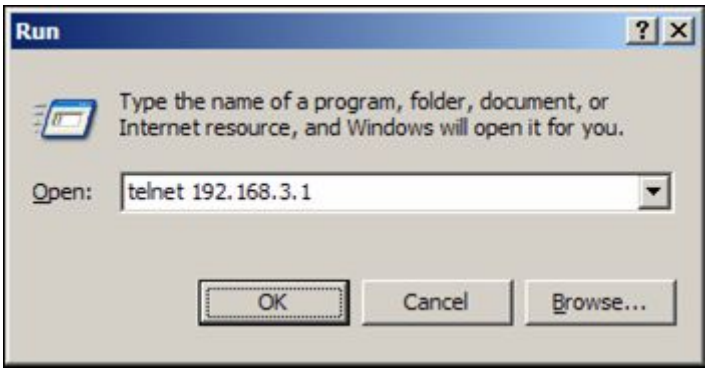
ii. Configure the Telnet login user name and password through the console port.

iii. Connect the host network port to the Ethernet port of the switch.

iv. Set the host IP address to one in the same network segment as that of the VLAN interface so that the host can ping the IP address of the VLAN interface.

v. Run the telnet command on the host and input the IP address of the VLAN interface to log in to the switch, as shown inFigure 7 .

FIGURE 7 RUN TELNET



vi. Click **OK** to enter the interface as shown inFigure 8 .

FIGURE 8 TELNET LOGIN

vii. Type the correct user name and password at the prompt to enter into switch configuration status.

Note:

i. ZXR10 5900/5200 allows up to four Telnet users at a time.

ii. Never modify/delete the IP address of the management Ethernet port during Telnet configuration through the management port; otherwise, the Telnet connection will be broken.

2. Telnet to the switch from other devices (such as a switch or router).
   i. Configure the IP addresses and interface of the VLAN through the console port.
   ii. Configure the Telnet login user name and password through the console port.
   iii. Consider router as an example. Connect the router and the switch, ensuring that the router can ping the IP address of the switch VLAN interface.
   iv. Run the telnet command on the router and input the IP address of the VLAN interface to log in to the switch.

SSH Connection Configuration

Telnet and FTP connections are not safe because they use the plain text to transmit the password and data on the network. This results in data to be easily intercepted by attackers. A disadvantage of the Telnet/FTP security authentication is that it is easily attacked by the man-in-the-middle. This imitates the server to receive the data sent by the client and imitates the client to transmit the data to the real server.

SSH can solve this hidden trouble. The SSH sets up a security channel for the remote login on non-security network and other network to encrypt and compress all transmitted data. In this way, no useful information can be obtained in the interception.

The current SSH protocol has two versions that incompatible each other: SSH v1.x and SSH v2.x. ZXR10 5900/5200 supports the SSH v2.0 that provides a safe remote login function.

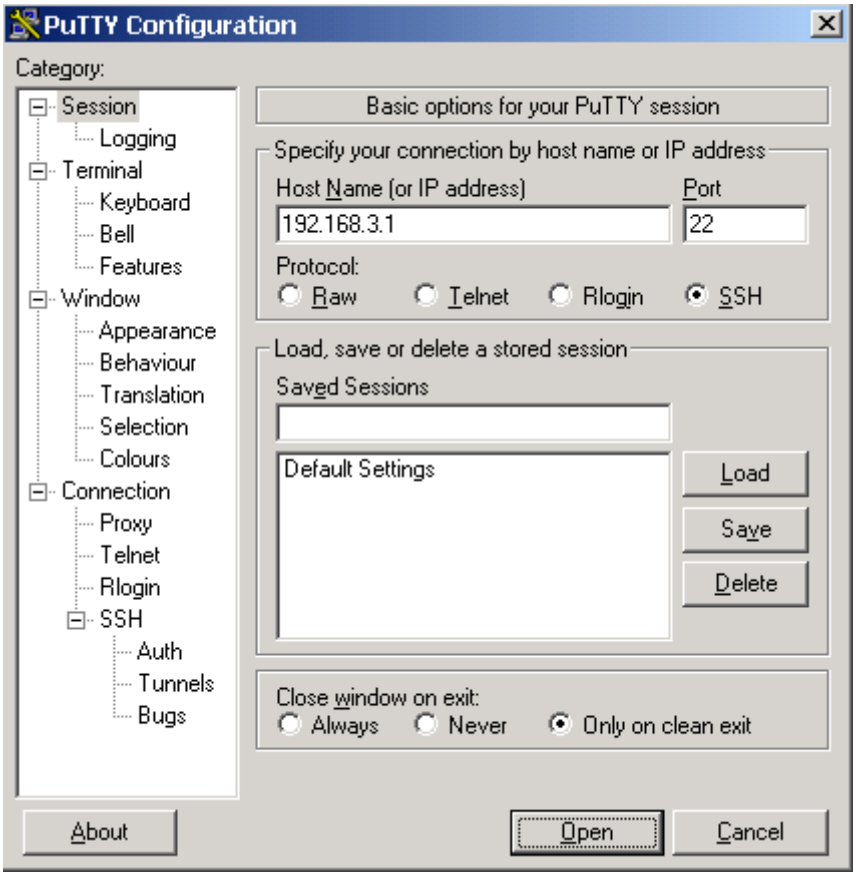
SSH consists of server and client, ZXR10 5900/5200 serves as SSH server and the host runs SSH client to log in to the switch.

1. Execute the following command to enable the SSH server in ZXR10 5900/5200. By default, SSH server function is disabled.

   ssh server enable

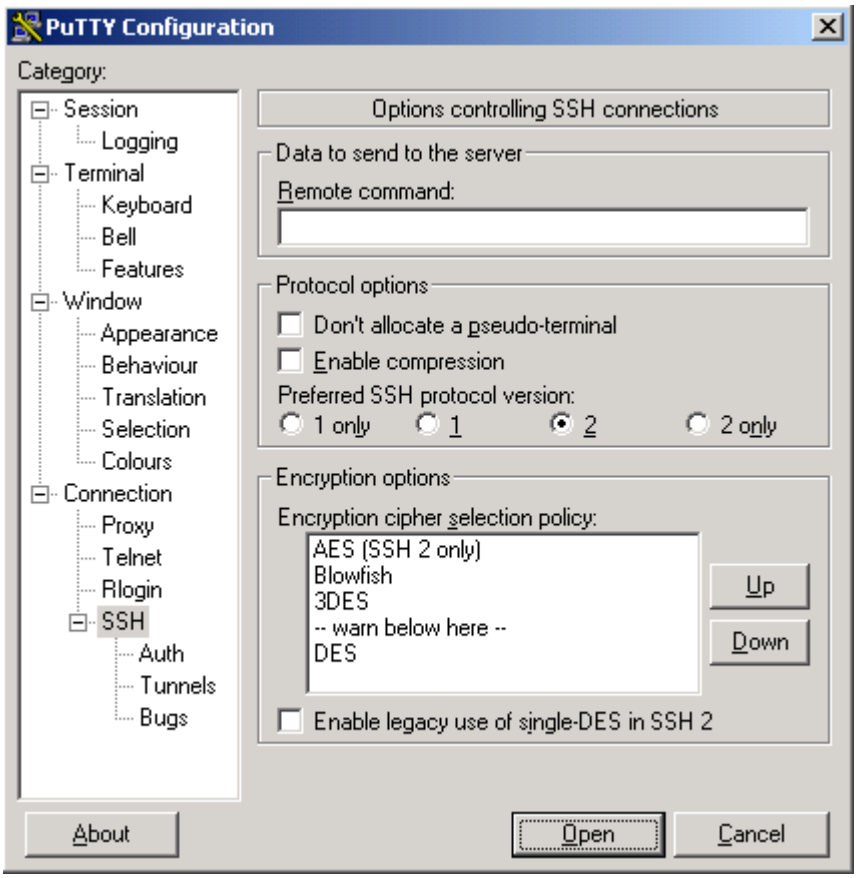
2. Connect the host network interface to the switch Ethernet interface so that the host can ping the IP of the switch VLAN interface.
3. Run the SSH client software (putty) on the host.
   i. Set the IP and port number of the SSH server, as shown inFigure 9 .

FIGURE 9 SETTING IP ADDRESS AND PORT NUMBER OF SSH SERVER



ii. Set the SSH version numberas shown in[Figure 10](#) .

FIGURE 10 SETTING THE SSH VERSION NUMBER



4. Click **Open** to log in to the switch and input the correct user name and password following the prompt.

The user enters switch configuration interface upon successful login.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is one of the most popular network protocols. An NM server can manage all devices on the network through this protocol.

SNMP adopts the management. That is based on the server and client. Background NM server serves as SNMP server and the foreground network device ZXR10 5900/5200 serves as the SNMP client. Foreground and background shares one MIB management database and the SNMP is used for communications.

NMS software supporting the SNMP shall be installed in the background NM server to manage and configure ZXR10 5900/5200.

Command Mode Function

ZXR10 5900/5200 allocates the commands to various modes based on the function. In order to authorize the facilitation to user's configuration and management for the switch only one command can be executed in the special mode.

Input a "?" mark in any command mode to view allowed commands in this mode. The main commands of the ZXR10 5900/5200 are shown in Table 2.

TABLE 2 COMMAND MODES

Mode	Prompt	Entry Command
User mode	`ZXR10>`	Directly enter it after logging in to the system
Privileged mode	`ZXR10#`	**enable** (user mode)
Global configuration mode	`ZXR10(config)#`	**configure terminal** (privileged mode)
Port configuration mode	`ZXR10(config-gei_1/x)#`	**interface** {<*interface-name*>|**byname** <*by-name*>} (global configuration mode)
VLAN database configuration mode	`ZXR10(vlan)#`	**vlan database**privileged mode
VLAN configuration mode	`ZXR10(config-vlan)#`	**vlan** {<*vlan-id*>|<*vlan-name*>} global configuration mode
VLAN interface configuration mode	`ZXR10(config-if)#`	**interface** {**vlan** <*vlan-id*>|<*vlan-if*>} global configuration mode
MSTP configuration mode	`ZXR10(config-mstp)#`	**spanning-tree mst configuration**global configuration mode
Standard ACL configuration mode	`ZXR10(config-std-acl)#`	**acl standard** {**number** <*acl-number*>| **name** <*acl-name*>}global configuration mode
Extended ACL configuration mode	`ZXR10(config-ext-acl)#`	**acl extended** {**number** <*acl-number*>| **name** <*acl-name*>}global configuration mode
L2 ACL configuration mode	`ZXR10(config-link-acl)#`	**acl link** {**number** <*acl-number*>| **name** <*acl-name*>}global configuration mode
Hybrid ACL configuration mode	`ZXR10(config-hybd-acl)#`	**acl hybrid** {**number** <*acl-number*>| **name** <*acl-name*>}global configuration mode
RIP configuration mode	`ZXR10(config-router)#`	**router rip**global configuration mode
RIP address configuration mode	`ZXR10(config-router-af)#`	**address-family ipv6 vrf** <*vrf-name*>RIP routing configuration mode
OSPF configuration mode	`ZXR10(config-router)#`	**router ospf** < *process-id*> global configuration mode

Mode	Prompt	Entry Command
IS-IS configuration mode	ZXR10(config-router)#	**router isis**global configuration mode
BGP configuration mode	ZXR10(config-router)#	**router bgp** <*as-number*> global configuration mode
BGP address configuration mode	ZXR10(config-router-af)#	**address-family** {**vpnv4** |{**ipv4 vrf** <*vrf-name*>}}BGP configuration mode
BGP configuration mode	ZXR10(config-router)#	**router pimsm**global configuration mode
Route map configuration mode	ZXR10(config-route-map)#	**route-map** <*map-tag*>[**permit**|**deny**][<*sequence-number*>]global configuration mode
Diagnosis test mode	ZXR10(diag)#	**diagnose**privileged mode

In any command mode, input a "?" mark behind the system prompt to view the list of available commands in this command mode.

In the privileged mode, execute the disable command to return to the user mode.

In the user mode and privileged mode, execute the exit command to exit the switch. In other command mode, execute the exit command to return to the previous mode.

In command modes other than the user mode and privileged mode, execute the end command or press**<Ctrl+z>**to return to the privileged mode.

Command Line Function

Online Help Command

1. Input a "?" mark behind the prompt of any command mode to view all commands and brief descriptions of this mode.

```
ZXR10>?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  login   Login as a particular user
  logout  Exit from the EXEC
  ping    Send echo messages
  quit    Quit from the EXEC
  show    Show running system information
  telnet  Open a telnet connection
  trace   Trace route to destination
  who     List users who are logining on
```

2. Input the question mark behind a character or character string to view the list of commands or keywords beginning with that

character or character string. There is no space between the character (character string) and the question mark.

```
ZXR10#co?
configure copy
ZXR10#co
```

3. Press **Tab** behind the character string. If the command or keyword beginning with this character string is unique. This will complete the character string with space at the end.

```
ZXR10#con<Tab>
ZXR10#configure    (there is a space between the configure and cursor.)
```

4. Input ? behind the command, keyword and parameter. It shows the keyword or parameter to be input next and its brief explanation. There is a space in front of the question mark.

```
ZXR10#configure ?
  terminal  Enter configuration mode
ZXR10#configure
```

5. If incorrect command, keyword or parameter is input, the error isolation is offered with ^ in the user interface after you press ENTER. The ^ is below the first character of the input incorrect command, keyword or parameter. An example is given below.

```
ZXR10#von ter
          ^
% Invalid input detected at ' ^'  marker.
ZXR10#
```

An example of system clock is given below.

```
ZXR10#cl?
clear  clock
ZXR10#clock ?
  set  Set the time and date
ZXR10#clock set ?
  hh:mm:ss  Current Time
ZXR10#clock set 13:32:00
% Incomplete command.
```

At the end of the above example, the system prompts that the command is not complete and other keyword or parameter should be input.

Note:

All commands in the command line operation are case-insensitive.

Command Abbreviation

ZXR10 5900/5200 allows the command or keyword to be abbreviated into a character or character string that uniquely identifies this command or keyword. For example, the **show** command can be abbreviated to **sh** or **sho**.

History Commands

The input command can be recorded in the user interface. Up to 10 history commands can be recorded and this function is useful for invoking a long or complicated command again.

Execute one of the following operations to re-invoke a command from the record buffer, as shown in Table 3.

TABLE 3 INVOKING A COMMAND

Command	Function
<Ctrl+P> or **<- >**	Invoke a history command in the buffer forward
<Ctrl+N> or **<¯>**	Invoke a history command in the buffer backward

In the privileged mode, execute the **show history** command to list the commands input the latest in this mode.

This page is intentionally blank.

Chapter 3

System Management

Table of Contents

File System

Introduction to File System

In ZXR10 5900/5200, FLASH is used as the major storage device for storing version files and configuration files. Operations, such as version upgrading and configuration saving, must be conducted in flash.

There are three directories in Flash by default.

1. IMGSystem mapping files (that is, image files) are stored under this directory. The extended name of the image files is .zar. The image files are dedicated compression files. Version upgrade means to change the corresponding image files under the directory.
2. CFGThis directory is for saving configuration files, whose name is startrun.dat. Information is saved in the Memory when using command to modify the switch configuration. To prevent the configuration information loss at the time of switch restart, use **write** command to write the information in the Memory into FLASH, and save the information in the startrun.dat file. When there is a need to clear the old configuration in the switch to reconfigure data, use **delete** command to delete startrun.dat file, then restart the switch.
3. DATAThis directory is for saving log.dat file which records alarm information.

Operating File System Management

ZXR10 5900/5200 provides many commands for file operations. Command format is similar to DOS commands as present in Microsoft Windows Operating System.

1. To copy files between Flash and FTP/TFTP server, use the following command.

   copy <*source-device*><*source-file*><*destination-device*><*destination-file*>

2. To view current directory path, use the following command.

   pwd

3. To view files and subdirectories of a specified device or under a specified directory, use the following command.

   dir [<*directory*>]

4. To delete a file under a designated directory of the current device, use the following command.

   delete <*filename*>

5. To enter into specific directory, use the following command.x

   cd <*directory*>

6. To make directory in flash, use the following command.

   mkdir<*directory*>

7. To delete a directory in flash, use the following command.

   rmdir<*directory*>

8. To modify the name of directory in flash, use the following command.

   rename <*source-filename*><*destination-filename*>

1. This example shows how to view the current files in the Flash.

```
ZXR10#dir
Directory of flash:/
       attribute    size       date         time  name
   1     drwx       512     MAY-17-2004  14:22:10 IMG
   2     drwx       512     MAY-17-2004  14:38:22 CFG
   3     drwx       512     MAY-17-2004  14:38:22 DATA
65007616 bytes total (48863232 bytes free)
ZXR10#cd img    /*Enter the directory img*/
ZXR10#dir       /*Show the current directory information*/
Directory of flash:/img
       attribute    size       date         time  name
   1     drwx       512     MAY-17-2004  14:22:10 .
   2     drwx       512     MAY-17-2004  14:22:10 ..
   3     -rwx  15922273     MAY-17-2004  14:29:18 ZXR10.ZAR
65007616 bytes total (48863232 bytes free)
```

2. This example shows how to create a directory ABC in the Flash and then delete it.

```
ZXR10#mkdir ABC /*Add a sub-directory of ABC in
 current directory*/
ZXR10#dir        /*view the information in current directory
and find the sub-directory of ABC*/
Directory of flash:/
       attribute    size       date         time  name
   1     drwx       512     MAY-17-2004  14:22:10 IMG
   2     drwx       512     MAY-17-2004  14:38:22 CFG
   3     drwx       512     MAY-17-2004  14:38:22 DATA
```

```
   4     drwx       512     MAY-17-2004  15:40:24 ABC
65007616 bytes total (48861184 bytes free)
ZXR10#rmdir ABC  /*remove the sub-directory of ABC*/
ZXR10#dir        /*Show the current directory information and
find sub-directory of ABC which has been removed*/
Directory of flash:/
       attribute    size       date         time  name
   1     drwx       512     MAY-17-2004  14:22:10 IMG
   2     drwx       512     MAY-17-2004  14:38:22 CFG
   3     drwx       512     MAY-17-2004  14:38:22 DATA
65007616 bytes total (48863232 bytes free)
```

FTP/TFTP Overview

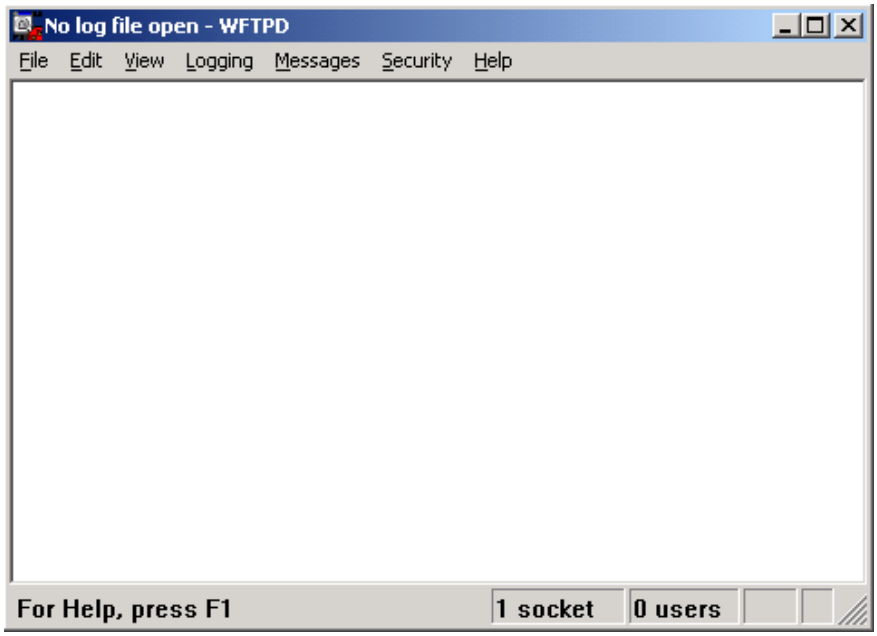
ZXR10 5900/5200 can server as an FTP/TFTP client. Files can be used as backup and restore purpose. Files can also be used as import/export configurations.

Configuring Switch as an FTP Client

Enable FTP server on the background host, and access the ZXR10 5900/5200 as an FTP client from the FTP server.

1. Run wftpd on the background host, and an interface as shownFigure 11 .

FIGURE 11 WFTPD INTERFACE



2. Select **Security**Select **User/Rights...**and perform the following operations on the popup dialog box:

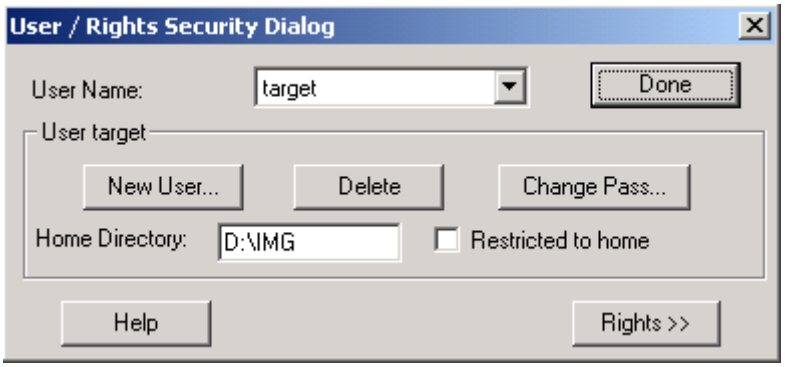
i. Click **New User...** to create a user, type target for an example, and set password for it

ii. Select target from the **User Name** drop-down list

iii. Type the directory of the version/configuration file in the **Home Directory** text box, such as D:\IMG.

After these setting, dialog box appears as shown in Figure 12 .

FIGURE 12 USER/RIGHTS SECURITY DIALOG BOX



3. Click **Done** to finish the settings.

Configuring Switch as an TFTP Client

Start TFTP server on the background host, and access the ZXR10 5900/5200 as a TFTP client from the TFTP server.

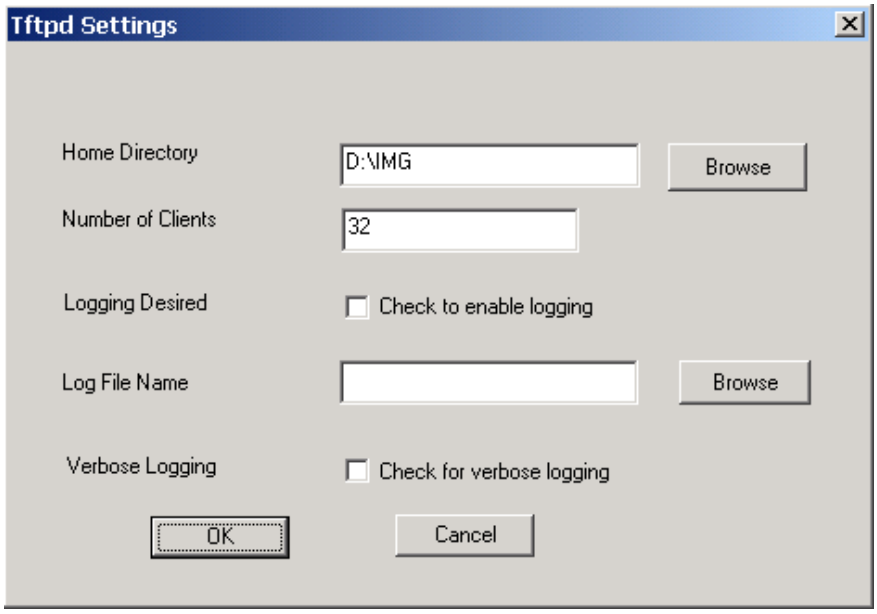
1. Run tftpd on the background host, and an interface as shown in Figure 13..

FIGURE 13 TFTPD INTERFACE

2. Select **Tftpd® Configure** click **Browse** on the popup dialog box and select a directory to store the version/configuration file, such as D:\IMG.

   The following dialog box will appear as shown in Figure 14 .

FIGURE 14 CONFIGURING DIALOG BOX



3. Click **OK** to finish the settings.

Background of TFTP server is implemented. Start the TFTP server, and run **copy** on the switch to backup/restore files or import/export configurations.

Backing up Data and Restoring Data

With FTP/TFTP, you can backup the software version file, configuration file and log file of ZXR10 5900/5200 to the background server, or restore backup files from the background server.

Backing Up Configuration File

After saving the configuration information to startrun.dat with the **write** command, you can backup the file to the background FTP/TFTP to keep the file intact and available for restoration.

Run the following command to back up the configuration file in the Flash to the background TFTP server:

```
ZXR10#copy flash: /cfg/startrun.dat
tftp: //168.1.1.1/startrun.dat
```

Restoring Configuration File

Run the following command to restore the backup of the configuration file from the background TFTP server:

```
ZXR10#copy tftp: //168.1.1.1/startrun.dat
 flash: /cfg/startrun.dat
```

Backing Up Version File

Take a backup of the running version file to the background server prior to version upgrade, so that the original version can be restored in case the new version loading fails. To backup the software version file is similar to backing up the configuration file.

Run the following command to backup the software version file in the Flash to img under the background TFTP server's root directory:

```
ZXR10#copy flash: /img/zxr10.zar
tftp: //168.1.1.1/img/zxr10.zar
```

Restoring Version File

Version restoration is to transfer the backup of the software version file from the background server to the foreground Flash of the switch over FTP/TFTP. Version restoration is important when the upgrade fails.

Procedure of version restoration is basically the same as version upgrade.

As mentioned previously, the ZXR10 5900/5200 supports configuration file import/export. Copy the configuration file startrun.dat to the background host over FTP/TFTP, where edit the file with a certain text editor, and then copy the file back to the foreground Flash's CFG directory over FTP/TFTP. The file will take effect the next time the system is rebooted.

Note:

1. When use **copy** command to transfer FTP file between back host and switch, fisrt configure host ip address in the same network segment that VLAN interface ip address is in and the interface which host connects belongs to the vlan and can ping through Vlan ip address.
2. Pay attention to the format requirement while editing startrun.dat with a text editor.

Software Version Upgrade

Normally, version upgrade is needed only when the original version does not support some functions or the equipment cannot run normally due to some special reasons. If version upgrade operations are performed improperly, upgrade failure may occur or the system fails to start. Therefore, before version upgrade, the maintenance personnel must be familiar with the principles and operations of the ZXR10 5900/5200 and learn the upgrade steps earnestly.

Upgrading the Version at Abnormality

To upgrade the version for ZXR10 5900/5200 in abnormal case, perform the following steps.

1. Set the switch management Ethernet port IP address and background host in the same network section.
2. Refer to FTP/TFTP Overview , start the background FTP server
3. Reboot ZXR10 5900/5200, and press any key at prompt in a HyperTerminal session to enter the Boot state. The display is as follows:

```
ZXR10 System Boot Version: 1.0
Creation date: Dec 31 2002, 14:01:52
(Omitted)
Press any key to stop for change parameters...
 2
[ZXR10 Boot]:
```

   Type "c" in the Boot state, and press ENTER to enter the parameter modification state. Change the boot mode to booting from the background FTP; change the FTP server address to that of the background host; change the client and gateway addresses

to that of the management Ethernet port of the switch; set the subnet mask and FTP user name and password pair. After the modification, the prompt ZXR10 Boot: appears.

```
[ZXR10 Boot]:c
’.’ = clear field;  ’-’ = go to previous field;  ^D = quit
Boot Location [0:Net,1:Flash] : 0
/*0 means booting from the background FTP, 1 means botting from Flash*/
Port Number                    : 24
Client IP [0:bootp]: 168.4.168.168
/*Management Ethernet port address*/
Netmask: 255.255.0.0
Server IP [0:bootp]: 168.4.168.89
/*Background FTP server address*/
Gateway IP: 168.4.168.168
/*Management Ethernet port address*/
FTP User: target
/*FTP user name target*/
FTP Password:
/*Password of target*/
FTP Password Confirm:
Boot Path: zxr10.zar     /*Default/
Enable Password:     /*Default*/
Enable Password Confirm:   /*Default*/
[ZXR10 Boot]:
```

4. Type @, and press ENTER. Then the system automatically boot from the background FTP server.

```
[ZXR10 Boot]:@
Loading...  get file zxr10.zar[15922273] successfully!
file size 15922273.
/*Omitted*/

**********************************************************
Welcome to ZXR10 5928 Switch of ZTE Corporation
**********************************************************
ZXR10>
```

5. If the system starts successfully, the user can use the **show version** command to check whether the new version is running in the memory. If not, booting from the background server failed. The user must repeat steps 1 to 5.
6. Delete the old version file (zxr10.zar) from the Flash’s IMG directory with the **delete** command. If there is enough space in the Flash, the user can reserve the old version with another name.
7. Copy the new version file on the background FTP server to the Flash’s IMG directory with the filename as zxr10.zar.
   i. Set temporary Vlan interface which is interworking with the host (suppose IP address is 168.4.168.1).
   ii. Set the host ip address (suppose ip address is 168.4.168.89) in the same network segment that Vlan interface ip address is in. The interface which host connects belongs to the vlan and can ping through Vlan ip address.
   iii. Use **copy** command at the privileged mode.

```
ZXR10#copy ftp: //168.4.168.89/zxr10.zar@target:target
 flash: /img/zxr10.zar
Starting copying file
.................................................................
.................................................................
.................................
file copied successfully.
ZXR10#
```

8. Check for the new version file in the Flash. If not found, the copying failed, when must repeat step 8 to copy the version again.
9. Reboot ZXR10 5900/5200, and follow step 4 to change the boot mode to booting from Flash, when Boot path changes to /flash/img/zxr10.zar automatically.

Note:

can also change the boot mode to booting form Flash with the **nvram imgfile-location local** command in the global configuration mode.

10. Type @ at the prompt ZXR10 Boot: and press ENTER to boot the system with the new version in the Flash.
11. When the system is booted successfully, check the running version to confirm the success of upgrade.

Upgrading the Version at Normality

Upgrade the software version in several different ways when the switch is working properly, including copying the version to the switch acting as an FTP/TFTP client and remote upgrade over FTP. The local upgrade procedure is as follows when the switch serving as an FTP client.

1. Connect the ZXR10 5900/5200's console port (on the main control board) to the serial port of the background host with a console cable attached to the switch; connect the management Ethernet port (10/100 M Ethernet port on the main control board) to the background host's network port with a straight through network cable. Make sure that both connections are correct.
2. Set the background host for upgrade to be in the network segment as the switch's management Ethernet port, so that the background host can ping the management Ethernet port.
3. Refer to FTP/TFTP Overview , Start the background FTP server
4. View the running version.
5. Use **Delete** command to the old version file from the Flash's IMG directory with the delete command. If there is enough space in the Flash, you can also reserve the old version with another name.
6. Copy the new version file on the background FTP server to the Flash's IMG directory with the filename as zxr10.zar.
7. Check for the new version file in the Flash's IMG directory. If the new version file is not found, the copy failed. The user must repeat step 5 to copy the version again.
8. When the system is rebooted successfully, check the running version to confirm the success of upgrade.

Configuring System Parameters

Setting a Hostname of System

The default hostname of system is ZXR10. Use **hostname** <*network-name*> in global configuration mode to modify the hostname .

Log on to router again after hostname modification and the prompt will include the new hostname.

Setting Welcome Message upon System Boot

Use **banner** to set welcome message upon system boot . Welcome message begins and ends with custom character. The example is as follows.

```
ZXR10(config)# banner incoming C
Enter TEXT message.  End with the character ' C' .
**********************************
    Welcome to ZXR10 Switch World
**********************************
C
ZXR10(config)#
```

Setting Privileged Mode Key

To prevent an unauthorized user from modifying the configuration, use the following command.

Command	Function
ZXR10(config)#**enable secret** {**0** <*password*>|**5** <*password*>|<*password*>}	This sets password.

Setting Telnet Username and Password

Command	Function
ZXR10(config)#**username** <*username*> **password** <*password*>	This sets Telnet user and password.

Setting System Time

Command	Function
ZXR10#**clock set** <*current-time*><*month*><*day*><*year*>	This sets system time.

Setting System Console User Connection Parameters

Command	Function
ZXR10(config)#**line console idle-timeout** <*idle-timeout*>	This sets idle-timeout time.
ZXR10(config)#**line console absolute-timeout** <*absolute-timeout*>	This sets absolute-timeout time.

Setting System Telnet User Connection Parameters

Command	Function
ZXR10(config)#**line telnet access-class** <*access-list-number*>	This configures access-class.
ZXR10(config)#**line telnet idle-timeout** <*idle-timeout*>	This configures dle-timeout time.
ZXR10(config)#**line telnet absolute-timeout** <*absolute-timeout*>	This configures absolute-timeout time.

There are parameters absolute-timeout and absolute-timeout after line console and line telnet. absolute-timeout refers to the time which is from the begin of connection to connection timeout. idle-timeout refers to the idle timeout that after user last operation. System will disconnect automatically when timeout. User should logon again if they need to continue operating switch system process. By default, absolute-timeout is 1440 minutes and idle-timeout is 120 minutes.

Allowing Multiple Users to Configure System at the Same Time

multi-user configure

be care for the reason that the configuration could bring switch configuration disorder.

Viewing System Information

Viewing Hardware and Software Versions of the System

The following information is displayed after carrying out **show version** command.

```
ZXR10#show version
ZXR10 Router Operating System Software, ZTE Corporation
ZXR10 ROS Version V4.08.23
ZXR10_5952 Software, Version ZXR10 5900 V2.8.23.A.12,
RELEASE SOFTWARE
Copyright (c) 2000-2007 by ZTE Corporation
Compiled Jun 14 2009, 11:47:14
System image files are flash:<//flash/img/zxr10.zar>
System uptime is 2 days, 18 hours, 19 minutes
[MPU]
Main processor: ZXR10 MPC8270, 450M - PCI with
256M bytes of memory
512K bytes of non-volatile configuration memory
16M bytes of processor board System flash (Read/Write)
ROM: System Bootstrap, Version: V1.12 , RELEASE SOFTWARE
Hardware Version: V1.8, CPLD Version: V1.4
System serial: 5952
```

Viewing Running Configuration

show running-config

Chapter 4

Interface Configuration

Table of Contents

Basic Port Configuration

The ZXR10 5900/5200 provides GE and XGE ports

- The GE electrical port supports full/half duplex, 10/100/1000 M adaptation and MDI/MDIX adaptation. It woks in auto-negotiation mode by default, consulting work mode and rate with the peer end.
- The GE optical port must work at 1000 M full duplex, it can't be configured duplex mode and rate but can be configured to work in the auto-negotiation mode.
- The XGE electrical port supports 10000M full duplex, it can't be configured to work in auto-negotiation, duplex mode and rate.
- The XGE optical port supports 10000M full duplex, it can't be configured to work in auto-negotiation, duplex mode and rate.

The system automatically adds ports: When you insert an interface board to a proper slot and start the board, ports of the board are automatically added to the port list.

Note:

The GE port and XGE port can't support hot swap.

ZXR10 5900/5200 names ports as follows:

<Port type>_<Slot No.>/<Port No.>

- *<Port type>* : gei (1000M Ethernet interface) and xgei (10000M Ethernet interface).
- *<Slot No.>*

  ZXR10 5924/5224 only has one slot.

  ZXR10 5928/5228/5928-FI/5228-FI/5952/5252 has 5 slots. There are 4 slots at the back of device. Slots numbered from

left to right are slot 2, slot 3, slot 4 and slot 5. Slot1 is GE port in front of the device.

- **<***Port No.***>**

  The No. of the port on the interface board, starting from 1.

  Example:

  - Gei_1/8 Port 8 on the GE interface board in slot 1.
  - Xgei_3/1 Port 1 on the XGE interface board in slot 3.

The ports are named differently because the number of boards and the number of ports on each board are different for specific devices.

1. ZXR10 5928/5228/5928-FI/5228-FI
   - The 24 ports in the front of the switch correspond to gei_1/1 to gei_1/24.
   - The 4 xgei Ethernet interface board at the back of switch are arranged from left to right, corresponding to xgei_2/1 xgei_3/1xgei_4/1xgei_5/1
2. ZXR10 5952/5252
   - The 48 ports correspond to gei_1/1gei_1/48.
   - The 4 xgei Ethernet interface board at the back of switch are arranged from left to right, corresponding to xgei_2/1 xgei_3/1xgei_4/1xgei_5/1
3. ZXR10 5924/5224
   - The 24 ports in the front of the switch correspond to gei_1/1 to gei_1/24.

Disabling/Enabling an Ethernet port

Step	Command	Function
1	`ZXR10(config)#`**interface** <*port-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**shutdown/no shutdown**	This disables/enables an Ethernet port.

shutdown command sets the physical link state of the port to down, when the port's link indicator goes off. All ports are enabled by default.

Enabling/Disabling Auto-Negotiation on an Ethernet Port

Step	Command	Function
1	ZXR10(config)#**interface** <*port-name*>	This enters interface configuration mode.
2	ZXR10(config--gei_1/x)#**negotiation auto/ no negotiation auto**	This enables/disables auto-negotiation on an Ethernet port.

Enable auto-negotiation on an Ethernet port when GE work on 1000M.

Configuring Automatic Negotiation Notification on an Ethernet Port

Command	Function
ZXR10(config-gei_1/x) #**negotiation auto** [**speed** [**10**|**100**]]	This configures automatic negotiation notification on an Ethernet port to 10M or 100M.

When working mode of PHY is electrical interface, GE, FE, 10M, half-duplex and full-duplex can be set if it can be notified.

When working mode of PHY is optical port, only half-duplex and full-duplex can be set if it can be notified. The notification of speed can't be set.

Description:

negotiation auto speed 100

negotiation auto speed 10

negotiation auto

no negotiation auto

The four are in mutual exclusive relationship.

After configuring nego auto speed 100|10, speed and duplex of port are not configured and only can be adaptive.

Setting Ethernet port Duplex Mode

Step	Command	Function
1	ZXR10(config)#**interface** <*port-name*>	This enters interface configuration mode.
2	ZXR10(config-gei_1/x)#**duplex** {**half**|**full**}	This sets Ethernet port to working in duplex mode.

Setting Ethernet Port Speed

Step	Command	Function
1	ZXR10(config)#**interface** <*port-name*>	This enters interface configuration mode.
2	ZXR10(config-gei_1/x)#**speed** {**10**|**100**}	This sets Ethernet port speed.

Only GE port allows configuration of its duplex mode and rate. Disable auto-negotiation on the port before the configuration.

Setting Flow Control on an Ethernet Port

Step	Command	Function
1	ZXR10(config)#**interface** <*port-name*>	This enters interface configuration mode.
2	ZXR10(config-gei_1/x)#**flowcontrol** {**enable**|**disable**}	This sets flow control on an Ethernet port.

Flow control is to restrict packet count sent to the Ethernet port within certain time period. The port sends a pause packet when the receive buffer is full to tell the remote port not to send any more packet to it within certain period. The Ethernet port can also receive pause packets from other devices and do as required by the packets.

Allowing/Prohibiting Jumbo Fame on an Ethernet Port

Step	Command	Function
1	`ZXR10(config)#`**interface** <*port-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**jumbo-frame**{**enable**|**disable**}	This allows/prohibits jumbo fame on an Ethernet port.

By default, maximum fame allowed on an Ethernet port is 1560-byte long and jumbo frames are prohibited. Maximum frame allowed on an Ethernet port is 9216-byte long when jumbo frame are permitted.

Setting Port Alias on an Ethernet Port

Step	Command	Function
1	`ZXR10(config)#`**interface** <*port-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**byname** <*by-name*>	This sets port alias on an Ethernet port.

Port alias is set to uniquely identify a port with a mnemonic name. Port can be accessed with its alias instead of the port name.

Setting Broadcast Storm Suppression on an Ethernet Port

Step	Command	Function
1	`ZXR10(config)#`**interface** <*port-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**broadcast-limit**<*value*>	This sets broadcast storm suppression on an Ethernet port.

Broadcast traffic through an Ethernet port can be limited. Broadcast packets are dropped when the traffic exceeds the limit so that the broadcast traffic through the Ethernet port is kept in a reasonable range. This effectively suppresses broadcast storm, helps avoid congestion and ensures normal provisioning of network ser-

vices. Broadcast storm suppression is implemented by setting the rate parameter, the lower the rate the smaller the allowed broadcast traffic.

Setting Multicast Packet Suppression on an Ethernet Port

Step	Command	Function
1	`ZXR10(config)#`**interface** <*port-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**multicast-limit** <*value*>	This sets multicast packet suppression on an Ethernet port.

When multicast packet suppression function of ZXR10 5900/5200 is enabled, port will take multicast packet suppression according to configured allowed number of multicast packet on an Ethernet port every second.

Setting Unknowcast Packet Suppression on an Ethernet Port

Step	Command	Function
1	`ZXR10(config)#`**interface** <*port-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**unknowcast-limit** < *value*>	This sets unknowcast storm suppression on an Ethernet port.

When unknowcast packet suppression function of ZXR10 5900/5200 is enabled, port will take unknowcast packet suppression according to configured allowed number of unknowcast packet on an Ethernet port every second.

Viewing Layer 2 Interface Physical Status

Short Description To view switch layer 2 physical interface running status such as if the interface is up, duplex, and rate.

Command	Function
ZXR10# **show interface brief**	This views interface running status.

Example The output of the viewing interface running status command is as follows.

```
ZXR10#show interface brief
Interface      portattribute  mode  BW(Mbits) Admin Phy   Prot Description
gei_2/1        electric   Duplex/full  1000   up    up    up    none
gei_2/2        electric   Duplex/full  1000   up    up    up    none
gei_2/3        electric   Duplex/full  1000   up    up    up    none
gei_2/4        electric   Duplex/full  1000   up    up    up    none
gei_2/5        electric   Duplex/full  1000   up    up    up    none
gei_2/6        electric   Duplex/full  1000   up    up    up    none
gei_2/7        electric   Duplex/full  1000   up    down  down  none
gei_2/8        electric   Duplex/full  1000   up    down  down  none
```

Admin, Phy, and Prot indicate management, physical, and protocol status of interface respectively. Only all three states are up, is interface in normal working status.

At the interface configuration mode, input **shutdown** , the Admin state of the interface will turn down.

lists some abnormal interface conditions and handling procedures.

TABLE 4 INTERFACE STATE ABNORMAL CONDITION

Interface State	Analysis and Solution
Admin is DOWN Phy is UP Prot is DOWN	This indicates that physical connection is normal and the corresponding interface maybe is shutdown, carry out the **no shutdown** command at the interface mode.
Admin is UP Phy is DOWN Prot is DOWN	This indicates that physical link has problem, check physical link.
Admin is UP Phy is UP Prot is DOWN	Check interface configuration , the problem maybe is that interface parameter is not correct or is not configured. refer to user manual to solve the problem. if this problem can’t be solved contact ZTE client supporting engineer for further handling.

Displaying Port Information

Command	Function
ZXR10#**show interface** [<*port-name*>]	This views Ethernet port state information.
ZXR10#**show running-config interface** <*port-name*>	This displays Ethernet port configuration information.

Example

1. It shows the state and statistics for port gei_1/2

```
ZXR10#show int gei_1/2
gei_1/2 is up, line protocol is up
Description is none
Keepalive set:10 sec
The port is electric
Duplex full
Mdi type:auto
VLAN mode is access, pvid 10 BW 100000 Kbits
Last clearing of "show interface" counters 0Day 0Hour 3Min 8Sec
120 seconds input rate : 0 Bps, 0 pps
120 seconds output rate: 0 Bps, 0 pps
Interface peak rate :
input 40 Bps, output 0 Bps
Interface utilization: input 0%, output 0%
/* Forward packets input/output statistics,
including error packet statistics  */
  Input:
    Packets      : 19                      Bytes     : 1501
    Unicasts     : 19                      Multicasts: 0
    Broadcasts   : 0                       Undersize : 0
    Oversize     : 0                       CRC-ERROR : 0
    Dropped      : 0                       Fragments : 0
    Jabber       : 0                       MacRxErr  : 0
  Output:
Packets      : 0                       Bytes     : 0
Unicasts     : 0                       Multicasts: 0
Broadcasts   : 0                       Collision : 0
LateCollision: 0

 Total:
    64B       : 0                          65-127B   : 19
    128-255B  : 0                          256-511B  : 0
    512-1023B : 0                          1024-2047B: 0
```

2. It shows the configuration information for port gei_1/2.

```
ZXR10#show run int gei_1/2
Building configuration...
interface gei_1/2
  negotiation auto
  switchport access vlan 10
  switchport qinq normal
```

Diagnosing and Analyzing Lines

ZXR10 5900/5200 supports cable connection diagnosis and analysis to find out any abnormality and accurately locate the fault for easy network management and troubleshooting.

FE electrical port and GE electrical port are both connected to other devices with a network cable. There are four twisted pairs in a network cable. There are four twisted pairs in a network cable. The FE electrical port uses pairs 1-2 and 3-6, and the GE electrical port uses all four pairs (1-2, 3-6, 4-5 and 7-8). Line detection is to test the state of each twisted pair, which includes:

1. Open: open line
2. Short: short circuit
3. Good: normal line
4. Broken: open/broken line
5. Unknown: unknown line or no result
6. Crosstalkline coupling
7. Fail: detection failure

In case of line fault, the location of failure is output. If the line is normal, the approximate length of the line is output. To diagnose and analyze a line, run the **show vct interface** command in any configuration modes other than user configuration mode.

Example: Detect the line of port gei_1/2.

```
ZXR10(config)#show vct int gei_1/2
CableStatus    Good
Pair           1-2       3-6       4-5       7-8
Status         Good      Good      Good      Good
Length         <50m      <50m      <50m      <50m
```

Caution:

Line diagnosis and analysis will restart the tested port, when links of the port is broken and then restored. This function is used only for faulty ports, and is not recommended for ports connected to users.

Port Mirroring Configuration

Port Mirroring Overview

Port mirroring is to copy data from one or more ports (mirrored ports) of a switch to a specified destination port (monitor port). This data is obtained from the mirrored port(s). It provides an effective tool for the maintenance and monitoring of the switch. Also it supports cross-equipment port mirroring (RSPAN).

Port mirroring function of ZXR10 5900/5200 complies with the following rules:

- Support up to one group of ports (eight mirrored ports to the most).
- Support cross-board port mirroring, that is, the mirrored port and monitor port can be on different interface boards.

- Support monitoring only sent/received data on the mirrored port.
- Support cross-equipment port mirroring (RSPAN), that is, mirrored port and monitor port can be on different equipment.

Configuring Port Mirroring

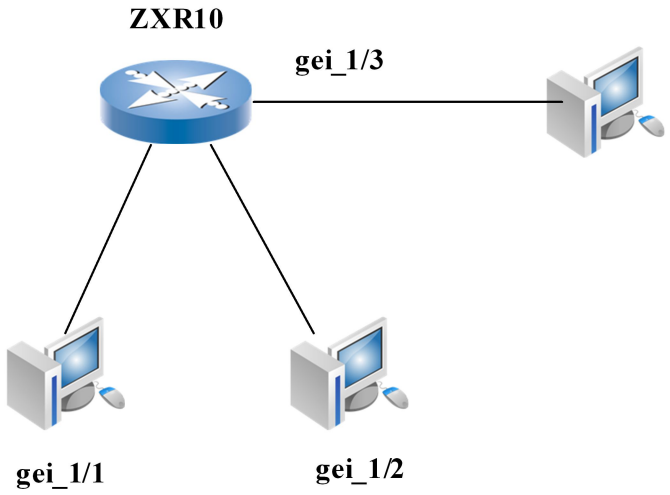
Step	Command	Function
1	ZXR10(config-gei_1/x)#**monitor session** <*session-number*> **source** [**direction** {**both**|**tx**|**rx**}]	This sets mirror port for capturing in/out traffic of monitor port.
2	ZXR10(config-gei_1/x)#**monitor session** <*session-number*> **desination**	This sets monitor port.
3	ZXR10(config-gei_1/x)#**monitor session** <*session-number*> **desination** [**rspan-vlanid** <*vlanid*>][**priority** < *priorityid* >]	This sets RSPAN monitor port.
4	ZXR10(config-gei_1/x)#**show monitor session** |<*session-number*>	This displays statistics of port mirroring.
5	ZXR10(config-gei_1/x)#**no monitor session**	This deletes port from port mirroring.

Port Mirroring Configuration Example

1. This example shows single device port mirroring configuration.

   Port gei_1/3 is connected to a computer, data received is on gei_1/1 and data received/sent is on gei_1/2 are to be monitored. This is shown in Figure 15.

FIGURE 15 PORT MIRRORING EXAMPLE



Configuration of switch:

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#monitor session 1 source direction rx
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#monitor session 1 source
ZXR10(config-gei_1/2)#exit
ZXR10(config)#interface gei_1/3
ZXR10(config-gei_1/3)#monitor session 1 destination
```

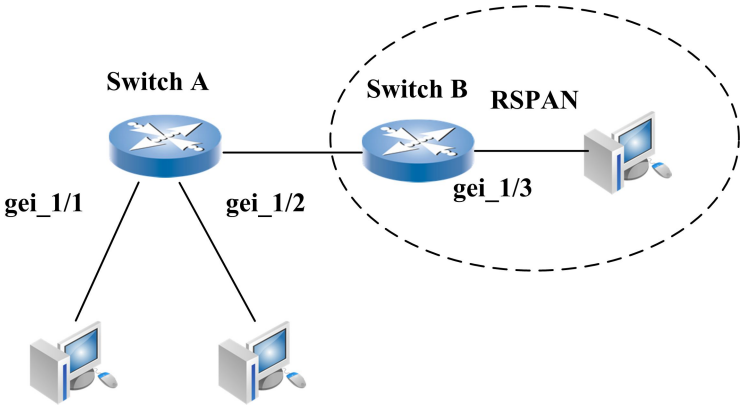
Show Port Mirroring Configuration:

```
ZXR10(config)#show monitor session 1
Session 1
-------------------------------------------------
Source Ports:
 Port: gei_1/1            Monitor Direction: rx
 Port: gei_1/2            Monitor Direction: both
Destination Port:
 Port: gei_1/3
 Rspan_vlanid : 0
 Rspan_priority: 0
-------------------------------------------------
ZXR10(config)#
```

2. The following example shows RSPAN mirroring configuration.

   As shown in Figure 16, port gei_1/3 is connected to other equipment's mirroring out port, data received is on gei_1/1 and data received/sent is on gei_1/2 are to be monitored, RSPAN's Vlan is Vlan 10 and the priority is 1.

FIGURE 16 PORT RSPAN MIRRORING EXAMPLE



Configuration of Switch A:

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#monitor session 1 source direction rx
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#monitor session 1 source
ZXR10(config-gei_1/2)#exit
ZXR10(config)#interface gei_1/3
ZXR10(config-gei_1/3)#monitor session 1 destination rspan-vlanid 10 priority 1
```

Loopback Detection Configuration

Port Loopback Detection Overview

ZXR10 5900/5200 supports single port loopback detection. This function can detect the loopback of user which connects to the switch and switch itself. Then it can solve this problem. It can avoid broadcast storm in result of loopback.

ZXR10 5900/5200 detects loopback of a few ports or all ports. By default it is not detected. It supports loopback detection in Vlan. One port supports up to loopback detection of 8 Vlans at the same time.

Configuring Port Loopback Detection

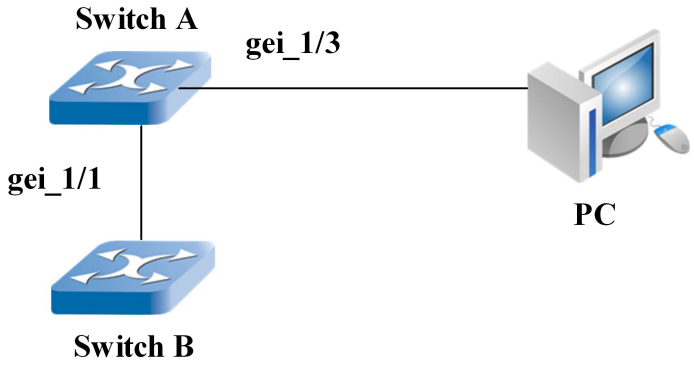
Step	Command	Function
1	ZXR10(config)#**loop-detect interface** <*port-name*>[**enable** | **disable**]	This enables the loopback detection function of one port or multiple ports.

Step	Command	Function
2	ZXR10(config)#**loop-detect interface** <*port-name*> **vlan** <*vlan-id*>[**enable** | **disable**]	This configures the loopback detection of Vlan in one port.
3	ZXR10(config)#**loop-detect protect-interface** <*port-name*><*enable* | **disable**>	This configures the loopback detection port interface. When a switch detects a loopback of one port, switch deal with it according to parameter protect-interface. When parameter protect-interface is enable, switch sets a alarm it has detected a loopback but there will be no operation. When the parameter protect-interface is disable, the switch will shutdown the port. After enabling loopback detection, the default parameter protect-interface is disable.
4	ZXR10(config)#**loop-detect reopen-time** <*interval*>	This configures the reopen-time when the port was shut down as a result of loopback detection.
5	ZXR10(config)#**show loop-detect interface**	This enables the loopback detection function.
6	ZXR10(config)#**show loop-detect interface-detail** <*port-name*>	This displays detail of port which enables loopback detection.
7	ZXR10(config)#**show loop-detect protect-interface**	This displays the port which enables loopback detection protection.
8	ZXR10(config)#**show loop-detect reopen-time**	This displays the reopen-time when one port has been shutdown in result of loopback detection.

Port Loop Detection Example

As shown in Figure 17, port gei_1/3 is connected to a computer, telnet into the switch A. Port gei_1/1 is in Vlan1 and Vlan2. Enable loopback detection in port gei_1/1. Loopback detection is done in Vlan1 and Vlan2 at the same time. Switch A is connected to Switch B with gei_1/1 port. Switch B shuts spanning-tree protocol and loop two ports with one network line. The two ports in loop and the port which connect to switch are in the same Vlans as gei_1/1.

FIGURE 17 PORT LOOPBACK DETECTION EXAMPLE



Configuration of Switch A:

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#switchport mode trunk
ZXR10(config-gei_1/1)#switchport trunk vlan 1-2
ZXR10(config-gei_1/1)#exit
ZXR10(config)#loop-detect interface gei_1/1 enable
ZXR10(config)#loop-detect protect-interface gei_1/1 enable
ZXR10(config)#loop-detect reopen-time 5
ZXR10(config)#loop-detect interface gei_1/1 vlan 1-2 enable
```

This displays detail of port which enables loopback detection.

```
ZXR10(config)#show loop-detect interface
gei_1/1
ZXR10(config)#show loop-detect interface-detail  gei_1/1
isUp            isMonitor      isLoop          isProtected
Yes              Yes             Yes             Yes
reopenTime      loopvlan       vlanRange
300                2               1-2
```

DOM Configuration

DOM Function Overview

DOMdigital optical monitoring is a part of optical module specification. The optical module with DOM function can read temperature, voltage, current, sending and receiving power of optical module. In addition, each optical module sets some threshold values of module (include alarm threshold and warning threshold) when leaving the factory. After DOM function is enabled, the module running state value can be polled by I2C bus of optical module. It is compared with threshold value. When the current value exceeds the threshold value that manufacturer sets, the alarm will be sent by syslog and SNMP trap.

Configuring DOM

Enabling DOM Function on Port

Command	Function
ZXR10(config-gei_1/x)#**optical-inform monitor** {**enable** | **disable**}	SFP DOM polling test function need to be enabled or disabled on interface by command line. The default is disabled. The polling diagnosis related information will be viewed after it is enabled. Otherwise the related optical module information can't be showed.

Only support physical interface, 100M port, gigabit port and 10G port.

Viewing Current Optical Module Information

Command	Function
ZXR10#**show optical-info brief**	This views brief information of interface optical module includes temperature, voltage, current, sending and receiving power. This supports single interface view and single board view.

Only support physical interface.

Example This views optical module information of an interface.

```
ZXR10#Show  optical-inform brief
                                                Optical    Optical
Interface   Temperature Voltage   Current   Tx Power   Rx Power
Name        (Celsius)   (Volts)   (mA)      (mW)       (mW)
-------------------------------------------------------------
gei_2/1/21  12.00       5.00      60.00     0.00       1.00
gei_2/1/22  12.00       5.00      60.00     0.00       1.00
gei_2/1/23  12.00       5.00      60.00     0.00       1.00
gei_2/1/24  12.00       5.00      60.00     0.00       1.00

ZXR10#Show  optical-inform brief  interface  gei_2/1/23
                                                Optical    Optical
Interface   Temperature Voltage   Current   Tx Power   Rx Power
Name        (Celsius)   (Volts)   (mA)      (mW)       (mW)
-------------------------------------------------------------
gei_2/1/23  12.00       5.00      60.00     0.00       1.00
```

The threshold is related to hardware optical module. If optical module and manufacturer are different the viewed information will be different.

Viewing Module Threshold Information

Command	Function
ZXR10#**show optical-inform detail** [**temperature voltage current rx-power tx-power**][**interface** <*interface-name*>]	This views detailed threshold information of interface optical module includes temperature, voltage, current, sending and receiving power. This supports single interface view and single board view.

Command parameter description+:

Parameter	Description
interface <*interface-name*>	interface name
temperature	Optical module temperature
voltage	Optical module voltage
current	Optical module current
rx-power	receiving power of optical module
tx-power	sending power of optical module

Only support physical interface.

Example This views threshold information of interface optical module.

```
ZXR10#show  optical-inform  detail  temperature
                        High Alarm  High Warn  Low Warn   Low Alarm
        Temperature  Threshold   Threshold  Threshold  Threshold
Port     (Celsius)    (Celsius)   (Celsius)  (Celsius)  (Celsius)
-------------------------------------------------------------
gei_1/1    48.1         100.0       100.0         0.0        0.0
gei_1/2    34.9         100.0       100.0         0.0        0.0

ZXR10#Show  optical-inform  detail  Voltage
                      High Alarm  High Warn  Low Warn   Low Alarm
          Voltage   Threshold   Threshold  Threshold  Threshold
Port     (Volts)      (Volts)     (Volts)    (Volts)    (Volts)
-----------------------------------------------------
gei_1/1    3.30          6.50        6.50      3.50      3.50
gei_1/2    3.30          6.50        6.50      3.50      3.50
```

The threshold is related to hardware optical module.If optical module and manufacturer are different the viewed information will be different.

Viewing the Record Information That Module Exceeds Threshold

Command	Function
ZXR10#**show optical-inform threshold-alarm** [**interface** <*interface-name*>]	This views threshold information of interface optical module includes temperature, voltage, current, sending and receiving power. This supports single interface view and single board view.

Only support physical interface.

Example This views alarm information that optical module exceeds threshold.

```
ZXR10#Show optical-inform threshold-alarm
Description:
tem : temperature       vol : volage   cur: current
tx  : transmit power    rx  : receive power
h-w : high-warning(+)   h-a : high-alarm(++)
l-w : low-warning(-)    l-a : low-alarm(--)
Interface Time in slot Threshold Violation Type(s) of Last Known
Name  (DDDD:HH:MM:SS)  (DDDD:HH:MM:SS) Threshold Violation
-------------------------------------------------------------
gei_2/1/22  14:57:27 04/29/2008 14:57:07 04/29/2008
 tem h-w -52.00C>=-52.00C
                 14:57:07 04/29/2008 vol h-w 5.00V>=5.00V
                 14:57:07 04/29/2008 cur l-w 60.00mA<=80.00mA
                 14:57:07 04/29/2008 rx l-a -440.00dBm<=-333.01dBm
                 14:57:07 04/29/2008 rx l-a -440.00dBm<=-333.01dBm
gei_2/1/23  14:57:27 04/29/2008 14:57:07 04/29/2008
tem h-w -52.00C>=-52.00C
                     14:57:07 04/29/2008 vol h-w 5.00V>=5.00V
                     14:57:07 04/29/2008 cur l-w 60.00mA<=80.00mA
                     14:57:07 04/29/2008 rx l-a -440.00dBm<=-333.01dBm
                     14:57:07 04/29/2008 rx l-a -440.00dBm<=-333.01dBm
```

The threshold is related to hardware optical module. If optical module and manufacturer are different the viewed information will be different.

This page is intentionally blank.

Chapter 5

Network Protocol Configuration

Table of Contents

IP Address Configuration

IP Address Overview

Network addresses in the IP protocol stack refer to IP addresses. IP address is composed of two parts: Network bit identifying the network to which this IP address belongs. Host bit identifying a certain host in the network.

IP addresses are divided into five classes: Class A, Class B, Class C, Class D and Class E. Classes A, B and C are the most common ones. Class D is the network multicast address and Class E is reserved for future use.Table 5lists range of each class.

TABLE 5 IP ADDRESS RANGE FOR EACH CLASS

Class	Prefix Characteristic Bit	Network Bit	Host Bit	Range
Class A	0	8	24	0.0.0.0~ 127.255.255.255
Class B	10	16	16	128.0.0.0~ 191.255.255.255
Class C	110	24	8	192.0.0.0~ 223.255.255.255

Class	Prefix Characteristic Bit	Network Bit	Host Bit	Range
Class D	1110	Multicast Address		224.0.0.0~ 239.255.255.255
Class E	1111	Reserved		240.0.0.0~ 255.255.255.255

Some Class A, B and C addresses are reserved for private networks. It is recommended that the internal network should use the private network address. These addresses refer to:

- Class A:10.0.0.0~10.255.255.255
- Class B:172.16.0.0~172.31.255.255
- Class C:192.168.0.0~192.168.255.255

This address classification method is to facilitate routing protocol designing. From this method it can be known the network type just by the prefix characteristic bit of the IP address. This method, however, cannot make the best of the address space. With the dramatic expansion of Internet, problem of address shortage becomes increasingly serious.

To make most of IP addresses, network can be divided into multiple subnets. Borrow some bits from the highest bit of the host bit as the subnet bit. Remaining part of the host bit still serves as the host bit. Thus, the structure of an IP address consists of three parts: Network bits, subnet bits and host bits.

The network bits and subnet bits are used to uniquely identify a network. Use the subnet mask to find which part in the IP address indicates network bits and subnet bits and which part stands for host bits. The part with subnet mask of "1" corresponds to the network bits and subnet bits of the IP address, while the part with subnet mask of "0" corresponds to host bits.

The division of the subnet greatly improves the utilization of IP address, and alleviates the problem of IP address shortage.

Regulations on IP addresses:

1. 0.0.0.0 is used when a host without an IP address is started. RARP, BOOTP and DHCP are used to obtain the IP address. The address serves as the default route in the routing table.
2. 255.255.255.255 is a destination address used for broadcast and cannot serve as a source address.
3. 127.X.X.X is called the loop-back address.
4. Only an IP address with host bits being all "0" indicate the network itself. An IP address with host bits being all "1" serves as the broadcast address of the network.
5. For a legal host IP address, the network part or the host part should not be all "0" or all "1".

Configuring IP Address

Step	Command	Function
1	ZXR10(config)#**interface** <*interface-name*>	This enters nterface configuration mode.
2	ZXR10(config-if-vlanX)#**ip address** <*ip-address*><*net-mask*>[<*broadcast-address*>][**secondary**]	This sets IP address.

One interface allows multiple IP addresses.

IP Address Configuration Example

Suppose that a layer 3 interface vlan1 is created on ZXR10 5900/5200. IP address to 192.168.3.1, and mask to 255.255.255.0 needs to be set. The detailed configuration is as follows:

```
ZXR10(config)#interface vlan 1
ZXR10(config-if-vlan1)#ip address 192.168.3.1 255.255.255.0
```

The **show ip interface** command can be used to view the IP address of the interface.

```
ZXR10(config-if-vlan1)#show ip interface

vlan1  AdminStatus is up, PhyStatus is up, line protocol is up
  Internet address is 10.1.1.1/24
  Broadcast address is 255.255.255.255
  IP MTU is 1500 bytes
  ICMP unreachables are always sent
  ICMP redirects are never sent
  ARP Timeout: 00:10:00
```

ARP Configuration

ARP Overview

Network device when sends data to another network device. It should know the IP address and physical address (MAC address) of the destination device. ARP is to map the IP address to the physical address, to ensure smooth communication.

At first, the source device broadcasts the ARP request with the IP address of the destination device. Then, all the devices on the network receive this ARP request. If one device finds the IP address in the request matches with its IP address, it sends a reply containing the MAC address to the source device. The source device obtains the MAC address of the destination device through this reply.

To reduce ARP packets on the network and send data faster, the mapping between IP address and MAC address is cached in the local ARP table. When a device wants to send data, it looks up the ARP table according to the IP address first. If the MAC address of the destination device is found in the ARP table, it is unnecessary to send the ARP request again. The dynamic entry in the ARP table will be automatically deleted after a period of time, which is called the aging time of the ARP.

Configuring ARP

Step	Command	Function
1	ZXR10(config)#**arp protect** {**interface** | **mac** | **whole**} **limit-num** <*number*>	This configures ARP protection.
2	ZXR10(config)#**arp to-static**	This sets dynamic arp entries to static arp.
3	ZXR10(config)#**interface vlan** <*vlan-id*>	This enters Layer 3 VLAN interface.
4	ZXR10(config-if-vlanX)#**arp timeout** <*timeout*>	This configures the aging time of ARP entry in the ARP buffer area.
5	ZXR10(config-if-vlanX)#**set arp** {**static**|**permanent** }<*ip-address*><*hardware-address*>	This adds arp entry in static/permanent binding.

To delete arp entry, use the following command.

Command	Function
ZXR10#**clear arp-cache interface**{**supervlan**<*id*>|**vlan**<*id*>}[<*ipaddress*>|**dynamic**|**permanet**|**static**]	This deletes all dynamic arp entries in from specific interface ARP buffer.

ARP Configuration Example

ARP configuration example is shown as follows.

```
ZXR10(config)#interface vlan 1
ZXR10(config-if-vlan1)#arp timeout 1200
```

ARP entry of designated interface can be viewed with **show arp** [<*interface-name*>] command.

The following example shows the ARP table of the layer 3 interface VLAN1.

```
ZXR10#show arp
Address   Age(min) Hardware Addr  Interface
10.1.1.1  -   000a.010c.e2c6  vlan1
10.1.100.100 18   00b0.d08f.820a  vlan1
10.10.10.2        S            0000.1111.2222       vlan1
10.10.10.3        P            0000.1111.2221       vlan1
ZXR10#
```

The "-"of Age in the result indicates that it is the ARP of the switch vlan interface. The arp is generated in the process of configuring switch vlan interface address. "s" indicates that it is a static ARP, and "P" indicates that it is a permanent ARP added manually. The number means the time since ARP updates last time.

This page is intentionally blank.

Chapter 6

Switch Stack System

Table of Contents

Switch Stack System Introduction

Switch stack system means the collection of multiple switches which is implemented by connecting the switch stack port with stack cable. The multiple switches in stack system work together as one switch. Layer 2 and Layer 3 protocols act as an entity in the network. 59 series switch support at most stack of 9 devices in which one switch is main device that can configure and manage all members in stack system.

All the features that main switch supports can be supported in stack system. Main switch saves configuration file of stack system. When configuration is saved, configuration fill will be copied to all stack member for backup. When stack system acts as layer 3 device, the MAC address of stack system is the unique ID in the network. The MAC address of main device in stack system is that of the whole stack system. Each stack member is identified by its stack member ID.

Any one of stack members can be main device. When main device isn't applicable, a new main device will be designated among other member devices according to a specific rule. The rule will be introduced as follows.

Stack system can be managed with a IP address which is not related to specific main device and other stack members but is a system level configuration. Even if main device or other stack members leave form stack system, stack system can be managed with this IP address.

There are two modes for managing stack system:

- The serial port cable is connected to any serial port of stack member. Management is implemented by CLI.
- Management is implemented by SNMP.

Member Specification of Switch Stack System

At most 9 devices compose a stack system by stack port. Each stack system only has one main device.

If an independent device enables stack it is stack system itself and the main device is itself. If two stack systems can be combined together an independent switch can be added into an existing stack system to increase the member number of this stack system.

If a stack member in the stack system is replaced by the switch with the same model and the member ID of this switch is same as that of the original stack member, this switch will implement the same configuration that is same as the configuration of replaced stack member.

When two running stack systems combine together, a main device will be selected from the two main devices for the reason that the two stack systems have their own main devices. The selection rule is same as the one that the main device is selected from stack members. The main device selected again and roles and configuration of all stack members in which the main device is. All members of the stack system which fails in selection will restart and join this stack system. During this joining process, these switch member IDs will possibly be allocated again. After joining, they will implement the configuration of the main device selected again.

If neither original main device nor original standby device is in the separate stack system all members of this stack system will restart. In addition, because the configuration of each stack system is same IP address will be in collision. IP address of the new stack system need to be modified. If the stack system is not be divided intentionally the operation is as follows:

1. Turn off powers of all switches in the new stack system.
2. Connect these switches with the original stack system.
3. Open the power of these switches.

Stack System Main Device Election and Renewed Election

Stack system main device election and renewed election will comply with the following rules:

1. The current switch is main device of stack system.
2. The switch member priority is the highest. When you want a switch to be the main device of stack system, configure its priority the highest.
3. The MAC address of the switch is the smallest when member priorities are same.

Main device will change when the following happen.

- The main device leaves from the current stack system.

- Main device restarts or powers off.
- Stack system is reset.*
- Other stack system is combined with the current stack system.*

As for the two conditions with *, the current main device will be joined into the process of main device renewed election and possibly be elected main device again.

When all switches in the stack system are opened or stack system is reset, only some stack members can join main device election. If stack member start time gap is in 15s it can join the main device election. Otherwise the device only can become stack member. All stack members can join the process of main device renewed election.

When the main device has been elected and the original main device has joined stack system again, the original main device can not be the current main device again but member device.

Stack System Member ID

Stack member ID , from 1 to 9, identifies each member in stack system. The interface configuration of each stack member is based on this member ID. Meanwhile, each stack member ID can be viewed by command line. If a device hasn't configured ID before joining stack system it will has default ID 1. In a stack system, two or multiple devices can't have the same IDs.

The command **nvram stack-machine-id** modifies stack device ID which is valid after restarting the device. When a device joins a stack system, if its ID is different from the ID of any member in this stack system the ID can be saved. Otherwise, it will be allocated the smallest and unused ID.

Stack System MAC Address

The MAC address of stack system uses that of main device. When main device leaves, the MAC address of main device which is newly elected will be the MAC address of stack system. MAC switch function sets MAC address switching time. If the device is configured this function, when main device leaves, the MAC address of stack system will be that of the original main device. At the setting time, if original main device returns to stack system again the MAC address of stack system will retain unchanged. Otherwise, it will be changed to the MAC address of new main device.

Stack Member Device Priority

The higher the switch priority, the greater the possibility of being main device during main device election. The priority range is

from 0 to 255. The default is 255. Priority information of all stack member devices can be viewed by **show switch all-status**.

The priority can be modified by **nvram stack-member-priority**. It can not be valid until the device restarts.

Stack Member Device Software Version Check and Automatic Upgrade

The software version in each member of stack system should be the same. When stack system starts and main device is elected, software version number of each member device will be automatically checked. If the version number of stack member is different from that of main device , the main device will synchronize the software to member device. After synchronizing, member device will restart and join the stack system again.

It is recommended that the priority of the device with the highest software version is configured the highest. Therefore it can be the main device and other member devices can automatically upgrades the latest software.

Stack System Configuration File

The configuration file of stack system applies configuration file of main device. The name of configuration file is stackcfg.dat. When system starts, it reads configuration file from flash of main device and recovers according to the record of this configuration file. When **write** is used, configuration file is not only saved in this device but also synchronized to other devices, that is , the same configuration file will be saved in flash of other devices. If member device leaves it will automatically load this configuration file after starting.

Stack System Active/Standby Changeover

There is a main device and a standby device in stack system (if there is only one device, that is main device). The command can be carried out in main device to configure the whole stack system. Meanwhile these configure will be synchronized to standby device, that is , the standby device will record these configuration. When main device has running fault or leaves, standby device will become main device and a new standby device will be elected from the rest of member devices. Therefore stack system configuration won’t lost and the effect on traffic forwarding will be minimized.

Configuring Switch Stack System

Step	Command	Function
1	ZXR10(config)#**mac switch-time** *<0-300>*	This configures time delayed parameter. The unit is second. The maximum value is 300s. 0, the default value, means when main device leaves MAC address is switched to new main device MAC address.
2	ZXR10(config)#**show running-config**	This views configured MAC switching time from the current configuration content. If this command is set mac switch-time will be viewed.

Reference Information

1. The function of enabling MAC switching.

   In stack system, the MAC address of main device is that of whole system. When main device leaves, standby device will be the main device. Meanwhile, its MAC address will replace MAC address of original main device to be that of the whole system. Now a time delay 1-300s can be configured by MAC switching function after device leaves. In this time, if the original main device joins this stack system again the MAC address of original main device will become that of stack system and whole system MAC address is not switched; If original main device doesn't join this stack system the MAC address of new main device will become that of stack system.

2. Default Configuration

Feature	Default Configuration
Enable/Disable stack	Disable
nvram stack-machine-id	1
nvram stack-member-priority	255
set interface stack-enable/stack-disable stack-port	Disable

Accessing the Specific Stack Member by Command Line

In stack system, all devices can log in to other devices by **session** to operate other devices. When logging in to member device, **show** operation or operation on file system will be carried out and configuring command operation can't be carried out. That mem-

ber device logging in to main device need the authentication of username and password which can be configured on main device.

Command	Function
ZXR10#**session** <*device id*>	The parameter is the ID of the device that will be log in to. After the command is carried out, the corresponding device can be operated.

Viewing Switch Stack System Information

Step	Command	Function
1	ZXR10#**show switch all-status**	This views the whole stack system information.
2	ZXR10#**show switch all-neighbours**	This views the whole stack system neighbor relationship.
3	ZXR10#**show switch neighbours stack-member-number**	This views neighbor relationship of designated device. The parameter is device ID.
4	ZXR10#**show switch stack-ports**	This views current device stack interface information including sending/receiving packet statistics.
5	ZXR10#**show switch stack-ports stack-member-number**	This views specific device stack interface information including sending/receiving packet statistics. The parameter is device ID.
6	ZXR10#**show switch status**	This views current device topology related content.
7	ZXR10#**show switch status stack-member-number**	This views designated device topology content. The parameter is device ID.

Chapter 7

ACL Configuration

Table of Contents

ACL Overview

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACL's can filter traffic as it passes through a router and permit or deny packets at specified interfaces.

An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACL's to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. It tests packets against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packets because the switch stops testing conditions after the first match. The order of conditions in the list is critical. If no conditions match, the switch rejects the packets. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet.

Packet matching rules defined by the ACL are also used in other conditions where distinguishing traffic is needed. For instance, the matching rules can define the traffic classification rule in the QoS.

ZXR10 5900/5200 provides the following six types of ACLs:

- Standard ACL: Only match the source IP address.
- Extended ACL: Match the following items: Source IP address, destination IP address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, ICMP type, ICMP Code, DiffServ Code Point (DSCP), ToS and Precedence.
- L2 ACL: Match source MAC address, destination MAC address, source VLAN ID, L2 Ethernet protocol type and 802.1p priority value.
- Hybrid ACL: Match source MAC address, destination MAC address, source VLAN ID, source IP address, destination IP ad-

dress, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number.

- Standard IPv6ACL: Only match the IPv6 source IP address.
- Extended IPv6ACL: Only match the IPv6 source and destination IP address.

Each ACL has an access list number to identify. The access list number is a number. The access list number ranges of different types of ACLs are shown as follows:

- standard ACL: 1~99
- Extended ACL: 100~199
- L2 ACL : 200~299
- Hybrid ACL: 300~349
- Standard IPv6ACL: 2000~2499
- Extended IPv6ACL : 2500~2999

Each ACL has at best 100 rules, with the rule number range from 1 to 100.

Configuring ACL

Configuring Time Range

Command	Function
`ZXR10(config)#`**time-range** *<timerange-name>*{*<hh:mm:ss>* **to** *<hh:mm:ss><days-of-the-week>*|**from** *<hh:mm:ss><mm-dd-yyyy>*[**to** *<hh:mm:ss><mm-dd-yyyy>*]}	This enables time range.

There are several conditions in time-range configuration.

- Configure time range for each day: Specify the exact start time and end time in a day.
- Configure period range: Specify the period to be a fixed day of a week.
- Configure date range: Specify start date and end date. If not configured, the start date is the day when configuration takes effect and the end date is the max day that system can identify.

Configuring ACL Rule

When configuring ACL, it is needed to enter ACL configuration mode firstly and then define ACL rules. The following items shall be noted when defining ACL rules:

1. If a packet matches multiple rules at the same time, the first matched rule shall apply. Therefore, the sequence of these rules is critical important. In usual cases, the rule with smaller range is put ahead and the rule with larger range is put behind.
2. Taking network security into account, an implicit Deny rule is automatically attached to the end of each ACL to deny all packets. Therefore, a Permit rule is usually configured at the end of ACL to permit all packets to pass through.

Configuring Basic ACL Rule

Step	Command	Function
1	ZXR10(config)#**acl standard** {**number** <*acl-number*>|**name** <*acl-name*>}	This enters the standard ACL configuration mode.
2	ZXR10(config-std-acl)#**rule** <*1-100*>{**permit**|**deny**}{<*source*>[<*source-wildcard*>]|**any**}[**time-range** <*timerange-name*>]	This configures the rules of ACL.
3	ZXR10(config-std-acl)#**move** <*rule-no*>{**after** | **before**}<*rule-no*>	This moves a rule behind of another rule.

Example This example defines a standard ACL. The ACL permits packets from the network segment 192.168.1.0/24 to pass, but reject packets with the source IP address of 192.168.1.100.

```
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 deny 192.168.1.100 0.0.0.0
ZXR10(config-std-acl)#rule 2 permit 192.168.1.0 0.0.0.255
```

Configuring Extended ACL

Step	Command	Function
1	ZXR10(config)#**acl extend** {**number** <*acl-number*>|**name** <*acl-name*>}	This enters the extended ACL configuration.
2	ZXR10(config-ext-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*source*><*source-wildcard*>|**any**}{<*dest*><*dest-wildcard*>|**any**}[<*icmp-type*>[**icmp-code** <*icmp-code*>]][{[**precedence** <*pre-value*>][**tos** <*tos-value*>]}|**dscp** <*dscp-value*>][**fragment**][**time-range** <*timerange-name*>]	This configures the rules based on ICMP.
3	ZXR10(config-ext-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*ip-number*>|**ip**}{<*source*><*source-wildcard*>|**any**}{<*dest*><*dest-wildcard*>|**any**}[{[**precedence** <*pre-value*>][**tos** <*tos-value*>]}|**dscp** <*dscp-value*>][**fragment**][**time-range** <*timerange-name*>]	This configures the rules based on IP or IP protocol number (excluded ICMP, TCP, UDP)
4	ZXR10(config-ext-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*source*><*source-wildcard*>|**any**}[<*rule*><*port*>]{<*dest*><*dest-wildcard*>|**any**}[<*rule*><*port*>][**established**][{[**precedence** <*pre-value*>][**tos** <*tos-value*>]}|**dscp** <*dscp-value*>][**fragment**][**time-range** <*timerange-name*>]	This configures the rules based on TCP.

Step	Command	Function
5	ZXR10(config-ext-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*source*><*source-wildcard*>|**any**}[<*rule*><*port*>]{<*dest*><*dest-wildcard*>|**any**}[<*rule*><*port*>][{[**precedence** <*pre-value*>][**tos** <*tos-value*>]}|**dscp** <*dscp-value*>][**fragment**][**time-range** <*timerange-name*>]	This configures the rules based on UDP.
6	ZXR10(config-ext-acl)#**move** <*rule-no*>{**after** | **before**}<*rule-no*>	This moves a rule behind another rule.

Example This shows an extended ACL to perform the following functions.

1. Permit UDP packets from the network segment 210.168.1.0/24, the destination IP address 210.168.2.10, the source port 100 and the destination port 200 to pass.
2. Forbid the BGP packets from the network segment 192.168.2.0/24 passing.
3. Forbid all ICMP packets.
4. Forbid all packets with the IP protocol No. 8.

```
ZXR10(config)#acl extend number 150
ZXR10(config-ext-acl)#rule 1 permit udp 210.168.1.0 0.0.0.255
 eq 100 210.168.2.10 0.0.0.0 eq 200
ZXR10(config-ext-acl)#rule 2 deny tcp 192.168.2.0 0.0.0.255
 eq bgp any
ZXR10(config-ext-acl)#rule 3 deny icmp any any
ZXR10(config-ext-acl)#rule 4 deny 8 any any
```

Configuring L2 ACL

Step	Command	Function
1	ZXR10(config)#**acl link number** <*acl-number*>	This enters the L2 ACL configuration mode.
2	ZXR10(config-link-acl)#**Rule** <*rule-no*>{**permit**|**deny**}<*protocol-number*|**any**>[**cos**<*value*>][**ingress** {<*source-mac*><*source-mac-wildcard*>|**any**}[**vlan-id** <*vlan*>]][**engress**{<*dest-mac*><*dest-mac-wildcard*>|**any**}][**time-range** <*timerange-name*>]	This configures the rules of ACL.
3	ZXR10(config-link-acl)#**move** <*rule-no*>{**after** | **before**}<*rule-no*>	This moves a rule behind another rule.

Example In this example, define a L2 ACL to permit IP packets with the source MAC address as 00d0.d0c0.5741 and the 802.1p as 5 from VLAN 10.

```
ZXR10(config)#acl link number 200
ZXR10(config-link-acl)#rule 1 permit any cos 5 douter 10
ingress 00d0.d0c0.5741 0000.0000.0000
```

Configuring Hybrid ACL

Step	Command	Function
1	ZXR10(config)#**acl hybrid** {**number** <*acl-number*>|**name** <*acl-name*>}	This enters the hybrid ACL configuration.
2	ZXR10(config-hybd-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*ip-number*>|**ip**}{<*source*><*source-wildcard*>|**any**}{<*dest*><*dest-wildcard*>|**any**}{[**any**|<*ether protocol*>]}[**cos** <*0-7*>][<*vlan-id*>][**ingress** <*source-mac*><*source-mac-wildcard*> **egress** <*dest-mac*><*dest-mac-wildcard*>][**time-range** <*timerange-name*>]	This configures the rules based on IP or IP protocol number (excluded ICMP, TCP, UDP).
3	ZXR10(config-hybd-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*source*><*source-wildcard*>|**any**}{[<*dest-ip*><*dest-wildcard*>| **any** {**ether-protocol**}[<*vlan-id*>][**cos**<*value*>][**egress** <*dst-mac*><*dst-wildcard*>][**ingress** <*sor-mac*><*sor-wildcard*>][**time-range**<*range-name*>]][**eq** <*port-number*>{<*dst-mac*><*dst-wildcard*>|**any**}<*ether-protocol*>[<*vlan-id*>][**cos**<*value*>][**egress**<*dst-mac*><*dst-wildcard*>][**ingress** <*sor-mac*><*sor-wildcard*>][**time-range** <*range-name*>]]}	This configures the rules based on TCP.
4	ZXR10(config-hybd-acl)#**rule** <*rule-no*>{**permit**|**deny**}{<*source*><*source-wildcard*>|**any**}{[<*dest-ip*><*dest-wildcard*>| **any** {**ether-protocol**}[<*vlan-id*>][**cos**<*value*>][**egress** <*dst-mac*><*dst-wildcard*>][**ingress** <*sor-mac*><*sor-wildcard*>][**time-range**<*range-name*>]][**eq** <*port-number*>{<*dst-mac*><*dst-wildcard*>|**any**}<*ether-protocol*>[<*vlan-id*>][**cos**<*value*>][**egress**<*dst-mac*><*dst-wildcard*>][**ingress** <*sor-mac*><*sor-wildcard*>][**time-range** <*range-name*>]]}	This configures the rules based on UDP.
5	ZXR10(config-hybd-acl)#**move** <*rule-no*>{**after** | **before**}<*rule-no*>	This moves a rule behind another rule.

Example This shows an extended ACL to perform the following functions:

1. Permit UDP packets from the network segment 210.168.1.0/24, the destination IP address 210.168.2.10, destination MAC address 00d0.d0c0.5741, the source port 100 and the destination port 200 to pass.
2. Forbid the BGP packets from the network segment 192.168.3.0/24 passing.
3. Forbid all packets with the MAC address 0100.2563.1425.

```
ZXR10(config)#acl hybrid number 300
ZXR10(config-hybd-acl)#rule 1 permit udp 210.168.1.0 0.0.0.255 Eq
100 210.168.2.10 0.0.0.0 eq 200 any Egress
 00d0.d0c0.5741 0000.0000.0000
ZXR10(config-hybd-acl)#rule 2 deny tcp 192.168.3.0 0.0.0.255
Eq BGP any any
ZXR10(config-hybd-acl)#rule 3 deny any any any ingress
 0100.2563.1425 0000.0000.0000
```

Configuring Basic IPV6 ACL

Step	Command	Function
1	ZXR10(config)#**ipv6 acl standard** {**number** <*acl-number*>|**name** <*acl-name*>}	This enters the basic ACL configuration mode.
2	ZXR10(config-std-v6acl)#**rule** <*1-100*>{**permit**|**deny**}{<*source*>|**any**}[**mac(**<*Source-mac*><*Source wildcard bits*>**)**][**time-range** <*timerange-name*>]	This configures the rules of ACL.
3	ZXR10(config-std-v6acl)#**move** <*rule-no*>{**after** | **before**}<*rule-no*>	This moves a rule behind another rule.

Example In this example, define a ACL to permit IP packets with the network segment as 10.0.0.0.0.0.0.0/16 to pass.

```
ZXR10(config)# ipv6 acl standard number 2000
ZXR10(config-std-v6acl)# rule  1 permit 10::/16
```

Configuring Extended IPV6 ACL

Step	Command	Function
1	ZXR10(config)#**ipv6 acl extended** {**number** <*acl-number*>|**name** <*acl-name*>}	This enters ACL configuration mode.
2	ZXR10(config-ext-v6acl)#**rule** <*1-maxRuleNo*>{**permit** | **deny**}{**(icmp** {<*source/prefix*>| **any**}{<*destination/prefix*>| **any**}**)** | **(**<*protocol*>{<*source/prefix*>| **any**}{<*destination/prefix*>| **any**}**)** | **(tcp**{<*source/prefix*>| **any**}[<*rule*>{<*0-maxPortNo*>|<*tcpporttype*>}]{<*destination/prefix*>| **any**}[<*rule*>{<*0-maxPortNo*>|<*tcpporttype*>}]**)** | **(udp**{<*source/prefix*>| **any**}[<*rule*>{<*0-maxPortNo*>|<*udpporttype*>}]{<*destination/prefix*>| **any**}[<*rule*>{<*0-maxPortNo*>|<*udpporttype*>}]**)**}[**ingress(**<*Source mac address*><*Source wildcard bits*>**)**][**egress(**<*Destination mac address*><*Destination wildcard bits*> **)**][{**time-range** <*timerange-name*>| **event** <*event-name*>}]	This configures the rules of ACL.
3	ZXR10(config-ext-v6acl)#**move** <*rule-no*>{**after** | **before**}<*rule-no*>	This moves a rule behind another rule.

Example In this example, define a extended ipv6 ACL to permit IP packets with the source ip network segment as 10.0.0.0.0.0.0.0/16 and destination ip network segment as 20.0.0.0.0.0.0.0/16 to pass and deny the packets with MAC address 0012.0001.0002 to pass.

```
ZXR10(config)# ipv6 acl extended 2500
ZXR10(config-ext-v6acl)# rule  1 permit 10::/16 20::/16
ZXR10(config-ext-v6acl)#rule 2 deny fragment any any ingress 0012
0001.0002  0000.0000.0000
```

Applying ACL on Physical Port

Step	Command	Function
1	ZXR10(config)#**interface** <*port-name*>	This enters interface configuration mode.
2	ZXR10(config-gei_1/x)#**ip access-group** <*acl-number*> **in**	This applies ACL on physical port.

Note:

One physical port only can apply one ACL. The new configuration will cover the old one. For example, on gei_1/1 configuration mode, the following two commands are configured.

ip access-group 10 in

ip access-group 100 in

Only ACL 100 takes effects.

Applying ACL on VLAN

ACL can be applied on both physical port and VLAN after it is defined.

Step	Command	Function
1	ZXR10(config)#**vlan** <*vlan-id*>	This enters VLAN configuration mode.
2	ZXR10(config-vlanX)#**ip access-group** {<*acl-number*><*acl-name*>} **in**	This applies ACL on VLAN.

Note:

1. Currently, ACL type that VLAN binds only supports IPv4 hybrid ACL
2. One VLAN can only apply one ACL, the new configuration will cover the old one. For example, in vlan configuration mode, the following two commands are configured

   ip access-group 300 in

   ip access-group 305 in

   only ACL 305 takes effects.

Configuring an ACL to Support Renaming

To configure a name for ACL rule, use the following commands.

Step	Command	Function
1	ZXR10(config)#**acl standard** {**number** <*acl-number*>|**name** <*acl-name*>}	This enters ACL configuration mode.
2	ZXR10(config-std-acl)#**rule** <*1-100*>{**permit**|**deny**}{<*source*>[<*source-wildcard*>]|**any**}[**time-range** <*timerange-name*>]	This configures the rules of ACL.
3	ZXR10(config-std-acl)#**rule-description** <*1-100*><*rule-description*>	This configures name for a rule.

Example: Define a standard ACL, permitting packets from network segment 192.168.1.0/24 to pass through and denying packets whose source IP addresses are 192.168.1.100. Rule 1 and rule 2 can be configured different name.

```
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 deny 192.168.1.100 0.0.0.0
ZXR10(config-std-acl)#rule-description  1 test1
ZXR10(config-std-acl)#rule 2 permit 192.168.1.0 0.0.0.255
ZXR10(config-std-acl)#rule-description  2 test2
```

Note:

Currently only IPv4 standard ACL, IPv4 extended ACL, IPv4 hybrid ACL and IPv4 layer 2 ACL support ACL renaming function.

ACL Configuration Example

A company has an Ethernet switch, to which users of both department A and department B and servers are connected. This is shown in Figure 18. The relevant provisions as follows:

1. Users of both department A and department B are forbidden to access the FTP server and the VOD server in work time (9:00–17:00), but can access the Mail server at any time.
2. Internal users can access the Internet through proxy 192.168.3.100, but users of department A are forbidden to access the Internet in work time.
3. General Managers of both department A and department B (with their IP addresses as 192.168.1.100 and 192.168.2.100 respectively) may access the Internet and all servers at any time.

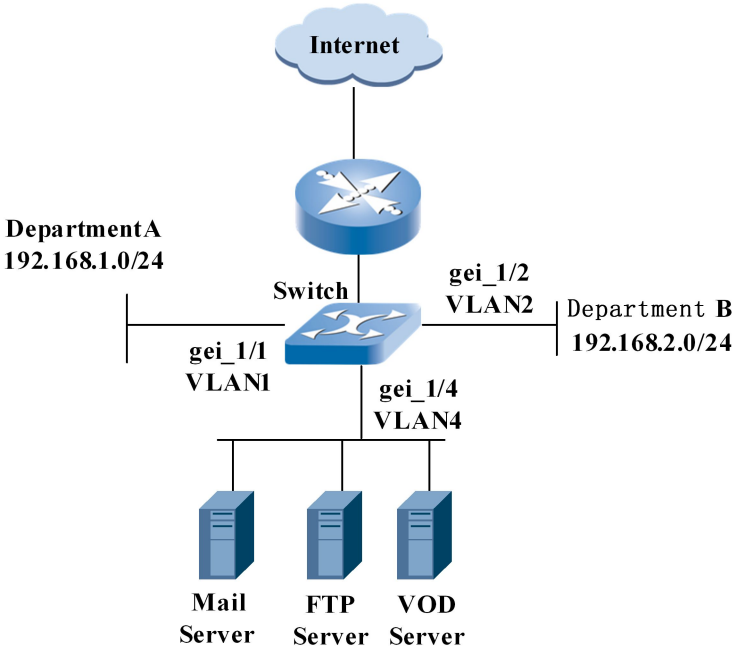
The IP addresses of the servers are as follows:

Mail server: 192.168.4.50

FTP server: 192.168.4.60;

VOD server: 192.168.4.70.

FIGURE 18 ACL CONFIGURATION EXAMPLE



Configuration of switch:

```
/*Configure time range*/
ZXR10(config)#time-range en
ZXR10(config)#time-range working-time
ZXR10(config-tr)#periodic daily 09:00:00 to  17:00:00

/*Define an extended ACL to limit users of department A*/
ZXR10(config)#acl extend number 100
ZXR10(config-ext-acl)#rule 1 permit ip 192.168.1.100 0.0.0.0 any
ZXR10(config-ext-acl)#rule 2 deny ip 192.168.1.0 0.0.0.255
192.168.4.60 0.0.0.0 time-range working-time
ZXR10(config-ext-acl)#rule 3 deny tcp any 192.168.4.70 0.0.0.0
time-range working-time
ZXR10(config-ext-acl)#rule 4 deny ip any 192.168.3.100 0.0.0.0
 time-range working-time
ZXR10(config-ext-acl)#rule 5 permit ip any any

/*Define an extended ACL to limit users of department B*/
ZXR10(config)#acl extend number 101
ZXR10(config-ext-acl)#rule 1 permit ip 192.168.2.100 0.0.0.0 any
ZXR10(config-ext-acl)#rule 2 deny ip 192.168.2.0 0.0.0.255
192.168.4.60 0.0.0.0 time-range working-time
ZXR10(config-ext-acl)#rule 3 deny tcp any 192.168.4.70 0.0.0.0
 time-range working-time
ZXR10(config-ext-acl)#rule 4 permit ip any any

/*Apply the ACL to the corresponding physical port*/
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#ip access-group 100 in
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#ip access-group 101 in
ZXR10(config-gei_1/2)#exit
```

ACL Maintenance and Diagnosis

For the convenience of ACL maintenance and diagnosis, ZXR10 5900/5200 provides related view commands.

1. To display the contents of all ACLs with specified list number, use the following command.

   show acl [<*acl-number*>|**name** <*acl-name*>]

2. To show whether an ACL is applied on a physical port, use the following command.

   show running-config interface <*port-name*>

Chapter 8

QoS Configuration

Table of Contents

QoS Overview

Traditional networks provide best-effort service, treating all packets identically and handling them with the first in, first out (FIFO) policy. This service policy delivers the packets to their destination as it can, without any assurance and guarantee for reliability and delivery delay, and so on for packet forwarding.

With the continuous emergence of new applications a new requirement for network service quality is raised because the traditional network at the best effort cannot satisfy the requirement for applications. For example, the user cannot use the VoIP service and real-time image transmission normally if packet transfer delay is too long. To solve the problem, provide the system with the capability of supporting QoS.

QoS is designed to provide different qualities of service for different demands from various applications, such as, providing specific bandwidth, reducing packet loss ratio, shortening packet transfer delay and delay-jitter. To achieve the above purposes, QoS offers the following functions:

1. Traffic classification
2. Traffic Policing
3. Traffic Shaping
4. Queue scheduling and default 802.1p Priority
5. Redirection and policy routing
6. Priority Mark
7. Flow Mirroring
8. Traffic statistics

Traffic Classification

Traffic refers to packets passing through switch. Traffic classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet.

Traffic classification of QoS is based on ACL and the ACL rule must be permit. The user can classify packets according to some filter options of the ACL which are as follows: Source IP address, destination IP address, source MAC address, destination MAC address, IP protocol type, TCP source port No. TCP destination port No., UDP source port No., UDP destination port No., ICMP type, ICMP code, DSCP, ToS, precedence, source VLAN ID, Layer 2 Ethernet protocol type and 802.1p priority value.

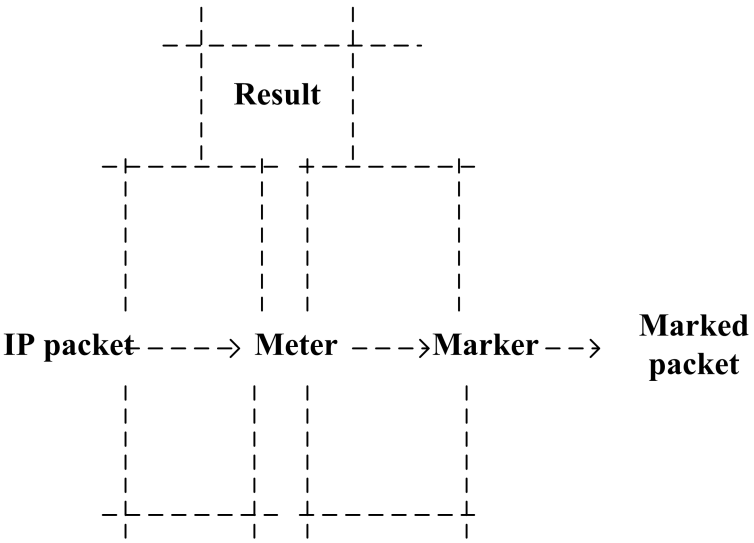
Traffic Policing

Traffic policing is to impose restriction on bandwidth occupied by some traffic flow to prevent it from exceeding specified bandwidth and thus affecting other services. As for the exceeding amount of traffics, conduct the following operation:

- Discard or forward
- Modify its DSCP value
- Modify its drop precedence (packets with higher drop precedence will be dropped preferentially when congestion occurs)

Traffic policing will not introduce extra delay. Its working process is shown in Figure 19.

FIGURE 19 TRAFFIC POLICING WORKING FLOW



ZXR10 5900/5200 implements the Single Rate Three Color Marker (SrTCM) (RFC2697) and Two Rate Three Color Marker (TrTCM) (RFC2698) functions, which both support the color-blind and color-aware modes.

It assumes that packets are colorless in color-blind mode but assumes that packets are marked in a color in color-aware mode. On the switch, each packet traversing the switch will be assigned a color according to some principle (packet information). Maker colors the IP packet according to result from Meter and the color is marked in DS field.

The following two methods will be described:

1. Single Rate Three Color Marker (SrTCM)

   This algorithm is used in Diffserv traffic conditioner. SrTCM measures data flow and marks packets according to three traffic parameters (Committed Information Rate, CIR; Committed Burst Size, CBS; Excess Burst Size, EBS). We call the three parameters as green, yellow and red marker respectively. A packet is green if its size is less than CBS. A packet is yellow if its size is between CBS and EBS and is red if its size exceeds EBS. By default, red packet is discarded.

2. Two Rate Three Color Marker (TrTCM)

   This algorithm is used in Diffserv traffic conditioner. TrTCM measures IP data flow and marks packets with green, yellow and red based on two types of rates (Peak Information Rate, PIR and Committed Information Rate, CIR) and their related committed burst size (CBS and PBS). A packet is marked in red if its size exceeds PIR. A packet is marked in yellow is its size is between PIR and CIR and is marked in green if its size is less than CIR.

Traffic Shaping

Traffic shaping is used to control the rate of output packets thus sending packets at even speed. Traffic shaping is used to match packet rate with downlink equipment to avoid congestion and packet discarding.

The difference between traffic shaping and traffic policing is that traffic shaping is to cache packets whose rate exceeds the limited value and send packets at even rate whereas traffic policing is to discard packets whose rate exceeds the limited value. Moreover, traffic shaping makes delay longer but traffic policing does not introduce any extra delay.

Queue Bandwidth Limit

Queue bandwidth limit means limiting the bandwidth of queue on interface to ensure the minimum bandwidth for queue. When traffic is blocked, certain bandwidth can be ensured for this queue.

Queue Scheduling and Default 802.1p

Each physical port of the ZXR10 5900/5200 supports eight output queues (queue 0 to queue 7) called CoS queues. The switch performs incoming port output queue operation according to the CoS queue corresponding to 802.1p of packets. In network congestion, the queue scheduling is generally used to solve the problem

that multiple packets compete with each other for resources at the same time.

ZXR10 5900/5200 supports Strict Priority (SP) and Weighted Round Robin (WRR) queue scheduling modes. Eight output queues of a port can adopt different modes respectively.

- SP Scheduling

  SP is to strictly schedule data of each queue according to queue priority. First send packets in the highest priority queue and after that, send packets in the higher priority queue. Similarly, after that, send packets in the lower priority queue, and so on.

  SP scheduling makes packets of key services processed preferentially, thus guaranteeing service quality of key services. But the low priority queue may never be processed and "starved".

- WRR

  WRR makes each queue investigated possibly and not "starved". Each queue is investigated at different time, that is, has different weight indicating the ratio of resources obtained by each queue. Packets in the high priority queue have more opportunities to be scheduled than the low priority queue.

Data priority is contained in the 802.1P label. If data entering the port is not marked with an 802.1P label, a default 802.1p value will be assigned by the switch.

Redirection and Policy Routing

Redirecting is used to make the decision again about the forwarding of packets with certain features according to traffic classification. Redirection changes transmission direction of packets and export messages to the specific port, CPU or next-hop IP address.

Redirect packets to the next-hop IP address to implement policy routing.

On the aspect of packet forwarding control, policy-based route has more powerful control capacity than traditional route because it can select a forwarding path according to the matched field in the ACL. Policy routing can implement traffic engineering to a certain extent, thus making traffic of different service quality or different service data (such as voice and FTP) to go to different paths. The user has higher and higher requirements for network performance, therefore it is necessary to select different packet forwarding paths based on the differences of services or user categories.

Priority Marking

Priority marking is used to reassign a set of service parameters to specific traffic described in the ACL to perform the following operations:

1. Change the CoS queue of the packet and change the 802.1p value.

2. Change the CoS queue of the packet and do not change the 802.1p value.
3. Change the DSCP value of the packet.
4. Change the discard priority of the packet.

Marking Outside Vlan Value

Marking outside Vlan value means configuring outside VLAN tag value for traffic complying with ACL rule.

Traffic Mirroring

Traffic mirroring is used to copy a service flow matching the ACL rule to the CPU or specific port to analyze and monitor packets during network fault diagnosis.

Traffic Statistics

Traffic statistics is used to sum up packets of the specific service flow. This is to understand the actual condition of the network and reasonably allocate network resources. The main content of traffic statistics contains the number of packets received from the incoming direction of the port.

Configuring QoS

Configuring Traffic Polices

Command	Function
ZXR10(config)#**traffic-limit in** <*acl-number*> **rule-id** <*rule-no*> **cir** <*cir-value*> **cbs** <*cbs-value*> **ebs** <*ebs-value*>[**pir** <*pir-value*>][**mode** <*mode*>][{[**drop -yellow**][**forward-red**][**remark-red-dp** {**high**|**low**|**me dium**}][**remark-red-dscp**<*value*>][**remark-yellow-dp** {**high**|**low**|**medium**}][**remark-yellow-dscp** <*value*>]}]	This configures traffic policy.

Color rendering configuration parameters contain cir, cbs, ebs and pir. To use the dual-rate marker algorithm, configure the pir parameter. The ebs parameter indicates the pbs parameter stipulated in the protocol.

Parameter **mode** <*mode*>: blind indicates Color-Blind mode and aware indicates Color-Aware mode.

Parameter **drop-yellow**: indicates dropping yellow packets; packets will be forwarded by default.

Parameter **forward-red**: indicates forwarding red packets; packets will be forwarded by default.

Parameter **remark** indicates remarking service parameter of packets with color:

- **remark-red-dp**: Remark drop precedence of red packets, priority parameter includes high, medium and low.
- **remark-red-dscp**: Remark DSCP priority of red packets, priority parameter is 0~63.
- **remark-yellow-dp**: Remark yellow packet dp to parameter of high, medium or low.
- **remark-yellow-dscp**:Remark yellow packet's dscp value from 0 to 63 and one value can be chosen..

Example This example shows the traffic policy of packets sent to the destination IP address of 168.2.5.5 on port of gei_1/1 and bandwidth is set to 10M.

```
ZXR10(config)#acl extended number 100
ZXR10(config-ext-acl)#rule 1 permit ip any
168.2.5.5 0.0.0.0
ZXR10(config-ext-acl)#exit
ZXR10(config)# traffic-limit in rule-id 1 cir
10000 cbs 2000 pir 10000 pbs 2000 mode blind
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#ip access-group 100 in
```

Configuring Traffic Shaping

Command	Function
ZXR10(config-gei_1/x)#**traffic-shape data-rate** <*rate-value*> **burst-size** <*value*>	This configures traffic shaping for the port.

Example This example shows the conduction of traffic shaping on port gei_1/1 and configures the port rate as 20 M.

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#traffic-shape data-rate  20000 burst-size 4
```

Configuring Queue Bandwidth Limit

Command	Function
ZXR10(config-gei_1/x)#**traffic-shape queue** <*queue-no*>{**max-datarate-limit** <*max-daterate-vlaue*>|**min-gua-datarate** <*min-datarate-vlaue*>}	This configures queue maximum and minimum bandwidth limit.

Example This example shows the conduction of queue bandwidth limit on port gei_1/1 and configures maximum bandwidth limit of queue 1 as 20M and minimum bandwidth as 2M, maximum bandwidth limit of queue 2 as 20M, minimum bandwidth limit of queue 3 as 2M.

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#traffic-shape queue 1 max-datarate-limit 20000
 min-gua-datarate 2000
ZXR10(config-gei_1/1)#traffic-shape queue 2 max-datarate-limit 20000
ZXR10(config-gei_1/1)#traffic-shape queue 3 min-gua-datarate 2000
```

Configuring Queue Scheduling and Default 802.1p of the Port

ZXR10 5900/5200 supports two types of queue scheduling modes: Strict Priority Scheduling (SP) and weighted Round-Robin (WRR). When these two modes are used together, SP has a higher priority than WRR.

Command	Function
ZXR10(config-gei_1/x)#**queue-mode strict-priority**|**wrr** <*Queue number*><*Queue weight*>	This configures queue scheduling and default 802.1p priority of the port.

Example This example shows the implementing of SP scheduling on the port gei_1/1. This implements WRR scheduling on port gei_1/2 and configures the weight of queue 0 to queue 7 sequentially as 10, 5, 8, 10, 5, 8, 9 and 10. Default 802.1p is configured on the port gei_1/2 as 5.

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#queue-mode strict-priority
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)# queue-mode wrr 0 10 1 5 2 8 3 10 4 5 5 8 6 9 7 10
ZXR10(config-gei_1/2)#priority 5
```

Configuring Redirection and Policy Routing

Command	Function
ZXR10(config)#**redirect in** <*acl-number*> **rule-id** <*rule-no*>{**cpu**|**interface** <*port-name*>|**next-hop** <*ip-address*>}	This redirects the packets.

Example This example shows the redirection of the packet whose source IP address is 168.2.5.5 on the port gei_1/4 to the port gei_1/3. In addition, it is to implement the policy routing to packet whose

destination IP address is 66.100.5.6 and specify the next-hop IP address as 166.88.96.56.

```
ZXR10(config)#acl extend number 100
ZXR10(config-ext-acl)#rule 1 permit ip 168.2.5.5 0.0.0.0 any
ZXR10(config-ext-acl)#rule 2 permit ip any 66.100.5.6 0.0.0.0
ZXR10(config-ext-acl)#exit
ZXR10(config)#redirect in 100 rule-id 1 interface gei_1/3
ZXR10(config)#redirect in 100 rule-id 2 next-hop 166.88.96.56
ZXR10(config)#interface gei_1/4
ZXR10(config-gei_1/4)#ip access-group 100 in
```

Configuring Priority Marking

Command	Function
ZXR10(config)#**priority-mark in** <*acl-number*> **rule-id** <*rule-no*>{ **dscp** <*dscp-value*>| **cos**<*cos-value*> **local-precedence** <*local-value*> **drop-precedence** <*dropl-value*>}}	This configures priority marking.

Example This example shows how to change the DSCP value of the packet whose source IP address is 168.2.5.5 on the port gei_1/1 to 34 and selects the output queue to 4.

```
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 permit 168.2.5.5
ZXR10(config-std-acl)#exit
ZXR10(config)#priority-mark in 10 rule-id 1 dscp 34 cos
 4  drop-precedence low
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#ip access-group 10 in
```

Configuring Outer VLAN Value

To configure outer VLAN value of traffic which matches ACL rule, use the following command.

Command	Function
ZXR10(config)#**qos set acl-svlan-map acl** {**acl-number** | **acl-name**} **rule** <*rule-id*> **to out-vlanid-**<*vlan-id*>	This configures outer VLAN value of traffic which matches ACL rule.

Example This example shows how to configure outer vlan value of traffic which complies with rule 1 on gei_1/4 as 2000.

```
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 permit 168.2.5.5
ZXR10(config-std-acl)#exit
ZXR10(config)#interface gei_1/4
ZXR10(config-gei_1/4)#ip access-group 10 in
ZXR10(config-gei_1/4)#exit
ZXR10(config)#qos set acl-svlan-map acl 10
 rule 1 to out-vlanid 2000
```

Configuring Traffic Mirroring

Command	Function
ZXR10(config)#**traffic-mirror in** <*acl-number*> **rule-id** <*rule-no*>{**cpu**|**interface** <*interface-num*>}	This configures traffic mirroring.

Example This example shows the mirror data traffic whose source IP address is 168.2.5.6 on the port gei_1/8 to the port gei_1/4.

```
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 permit 168.2.5.5
ZXR10(config-std-acl)#rule 2 permit 168.2.5.6
ZXR10(config-std-acl)#exit
ZXR10(config)#traffic-mirror in 10 rule-id 2 interface gei_1/4
ZXR10(config)#interface gei_1/8
ZXR10(config-gei_1/8)#ip access-group 10 in
ZXR10(config-gei_1/8)#exit
```

Configuring Tail-Drop

Command	Function
ZXR10(config)#**qos tail-drop** < *session-index*> **queue-id** < *queue-id*>< *all-threshold*>< *yellow-threshold*>< *red-threshold*>	This configures the tail-drop parameter.

To enable the tail-drop function on the port, use the following command.

drop-mode tail-drop <*session-id*>

Example This example shows the configuration of tail-drop. In queue 1: Red packets tail-drop value is 120. Yellow packets tail-drop value is 120. all packets tail-drop value is 240. This is configured on the port gei_1/8.

```
ZXR10(config)#qos tail-drop 1 queue-id 1 240 120 120
ZXR10(config)#interface gei_1/8
ZXR10(config-gei_1/8# drop-mode tail-drop 1
```

Configuring Traffic Statistics

Command	Function
ZXR10(config)#**traffic-statistics** < *acl-number*> **rrulle-iid** < *rule-no*> **pkt-type** { **all**| **green**| **red**| **yellow**} **statistics-type** { **byte**| **packet**}	This configures traffic statistics.

Example This example shows the conduction of traffic statistics to data whose destination IP address network segment is 67.100.88.0/24 on the port gei_1/8.

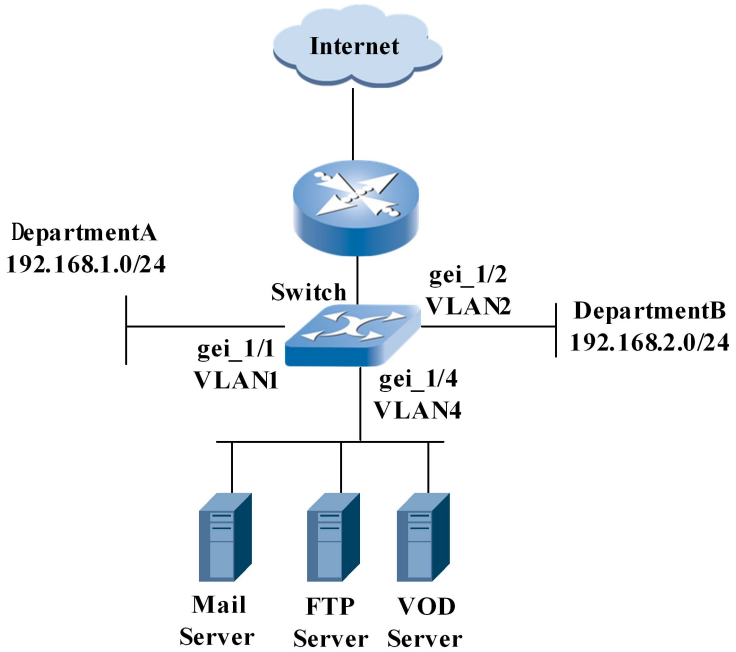
```
ZXR10(config)#acl extend number 100
ZXR10(config-ext-acl)#rule 1 permit ip 168.2.5.5 0.0.0.0 any
ZXR10(config-ext-acl)#rule 2 permit ip any 67.100.88.0 0.0.0.255
ZXR10(config-ext-acl)#exit
ZXR10(config)#traffic-statistics 100 rule-id 2 pkt-type all statistics-type byte
ZXR10(config)#interface gei_1/8
ZXR10(config-gei_1/8)#ip access-group 100 in
```

QoS Configuration Example

Typical QoS Configuration Example

Network A, Network B and internal servers are all connected to an Ethernet switch, as shown in Figure 20. One of internal servers is the VOD server with the IP address of 192.168.4.70. To guarantee service quality of the VOD, configure it as one with high priority. The internal user can access the Internet over the agent 192.168.3.100 but the bandwidth of Network A and Network B should be restricted and their traffic statistics should be conducted.

FIGURE 20 QOS CONFIGURATION EXAMPLE



Switch configuration:

```
ZXR10(config)#acl extend number 100
ZXR10(config-ext-acl)#rule 1 permit tcp any 192.168.4.70 0.0.0.0
ZXR10(config-ext-acl)#rule 2 permit ip any 192.168.3.100 0.0.0.0
ZXR10(config-ext-acl)#rule 3 permit ip any any
```

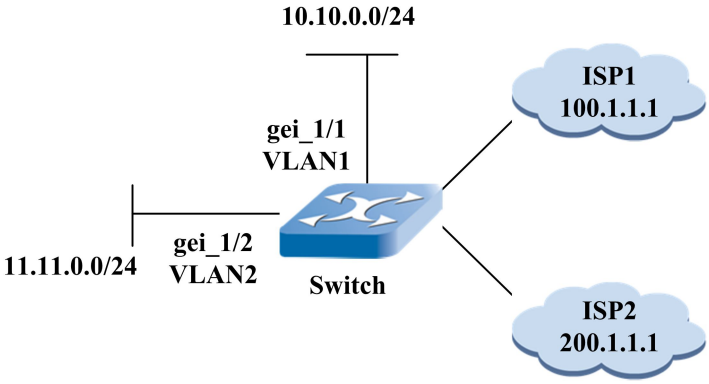
```
ZXR10(config-ext-acl)#exit
/*To guarantee the service quality of the VOD, change the
 802.1pvalue to 7*/
ZXR10(config)#priority-mark in 100 rule-id 1 dscp 62
 cos 7 local-precedence 7  drop-precedence low
/*Restrict the bandwidth of Network A to access Internet*/
ZXR10(config)#traffic-limit in 100 rule-id  2 cir 5000
 cbs 2000 ebs 3000 mode blind
/*Sum up traffic of Network A*/
ZXR10(config)#traffic-statistics in 100 rule-id 2
 pkt-type all statistics-type byte

ZXR10(config)#acl extend number 101
ZXR10(config-ext-acl)#rule 1 permit tcp
192.168.2.0 0.0.0.255 192.168.4.70 0.0.0.0
ZXR10(config-ext-acl)#rule 2 permit ip any
192.168.3.100 0.0.0.0
ZXR10(config-ext-acl)#rule 3 permit ip any any
ZXR10(config-ext-acl)#exit
/*To guarantee the sevice quality of the VOD, cange the
802.1p value to7*/
ZXR10(config)#priority-mark in 101 rule-id 1 dscp 62
 cos 7 drop-precedence low
/*Restrict the bandwidth of Network B to access Internet*/
ZXR10(config)#traffic-limit in 101 rule-id 2 cir 10000
cbs 2000 ebs 3000 mode blind
/*Sum up traffic of Network B*/
ZXR10(config)#traffic-statistics in 101 rule-id 2
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#ip access-group 100 in
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#ip access-group 101 in
```

Policy Routing Configuration Example

When there are many Internet Service Provider (ISP) egresses on the network, select different ISP egresses for users from different groups through policy routing or select different ISP egresses based on service types.

As shown in Figure 21, Users on both sub-networks are connected to the switch and there are two available ISP egresses. It is required to select different egresses based on IP addresses of users as follows: Users on the sub-network 10.10.0.0/24 use the ISP1 egress. Users on the sub-network 11.11.0.0/24 use the ISP2 egress.

FIGURE 21 POLICY ROUTING EXAMPLE



Switch configuration:

```
/*Define an ACC, which describes users in 10.10.0.0/24
network segment and 11.11.0.0/24 network segment*/
ZXR10(config)#acl standard number 10
ZXR10(config-std-acl)#rule 1 permit 10.10.0.0 0.0.0.255
ZXR10(config-std-acl)#rule 2 permit 11.11.0.0 0.0.0.255
ZXR10(config-std-acl)#exit

/*Configure policy routing of QoS*/
ZXR10(config)#redirect in 10 rule-id 1 next-hop 100.1.1.1
ZXR10(config)#redirect in 10 rule-id 2 next-hop 200.1.1.1

/*Apply to the corresponding port*/
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#ip access-group 10 in
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#ip access-group 10 in
```

QoS Maintenance and Diagnosis

ZXR10 5900/5200 provides the following commands of QoS maintenance and diagnosis.

1. To display QoS configuration, use the following command.

   show qos

2. To displayconfiguration of map of service parameter of data packets according to conformance level and DSCP, use the following command.

   show qos conform-dscp

3. To display 802.1p parameter map table configuration information according to local-precedence, use the following command.

   show qos cos-local-map

4. To display table configuration information that 802.1P user priority maps to switch local precedence, use the following command.

   show qos cos-drop-map

Example

```
ZXR10(config)#acl standard number 1
ZXR10(config-std-acl)#rule 1 permit 100.1.1.1
ZXR10(config-std-acl)#exit
ZXR10(config)#traffic-limit in 1 rule-id 1 cir 10000 cbs 2000
 ebs 2000 mode blind
ZXR10(config)#show qos

traffic-limit in 1 rule-id 1 cir 10000 cbs 2000 ebs 2000 mode blind

ZXR10(config)#qos conform-dscp 1 0 7 2
ZXR10(config)#show qos conform-dscp

qos conform-dscp 1 0 7 2

ZXR10(config)#qos cos-local-map 1 2 3 4 5 6 7 0
ZXR10(config)#show qos cos-local-map

qos cos-local-map 1 2 3 4 5 6 7 0

ZXR10(config)#qos cos-drop-map  2 1 0 2 1 1 0 1
ZXR10(config)#show qos cos-drop-map

qos cos-drop-map 2 1 0 2 1 1 0 1
```

This page is intentionally blank.

Chapter 9

DHCP Configuration

Table of Contents

DHCP Overview

Dynamic Host Configuration Protocol (DHCP) enables a host on the network to obtain an IP address ensuring its normal communication and relevant configuration information from a DHCP server.

DHCP adopts UDP as the transmission protocol. Host sends a message to Port 67 of the DHCP server and the DHCP server returns the message to Port 68 of the host. The DHCP works in the following steps:

1. Host sends a broadcast packet DHCPDiscover including the request of IP address and other configuration parameters.
2. DHCP server returns a unicast packet DHCPOffer including the valid IP address and configuration.
3. Host selects the server which returns DHCPOffer arriving at first and sends a unicast DHCPRequest to the server, indicating to accept relevant configuration.
4. Selected DHCP server returns a unicast packet DHCPAck for confirmation.

By now the host can use the IP address and relevant configuration obtained from the DHCP server for communication.

DHCP supports three mechanisms for IP address allocation:

1. Automatic allocation—DHCP assigns a permanent IP address to a client.
2. Dynamic allocation—DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
3. Manual allocation—the network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

Usually Dynamic allocation method is adopted. The valid time segment of using the address is called lease period. Once the lease period expires, the host must request the server for continuous lease. The host cannot continue to lease until it accepts the request, otherwise it must give up unconditionally.

Routers do not send the received broadcast packet from a sub-network to another by default. But the router as the default gateway of the client host must send the broadcast packet to the sub-network where the DHCP server locates when the DHCP server and client host are not in the same sub-network. This function is called DHCP relay.

ZXR10 5900/5200 can act as a DHCP server or DHCP relay to forward DHCP information but it cannot use both functions at the same time.

DHCP makes IP address allocation more convinent. But with the wide application of DHCP service, some problem happens. Firstly, DHCP service allows multiple DHCP servers to be in a subnet, which means that administrator can't assure that client doesn't get IP address from illegal DHCP server set by some clients but only gets legal IP address from DHCP server set by administrator. Secondly, in subnet deployed DHCP service, the host which is designated legal IP address, subnet mask and gateway can access network normally. But DHCP server will still allocate this IP address to other hosts possibly. It will lead to address collision and affect the normal distribution of IP address. DHCP snooping function is enabled for ZXR10 5900/5200 to prevent bogus DHCP server from being laid in network, and in this case, the port connecting to DHCP server must be set to trusted port. What's more, dynamic ARP inspection technology can be used together to prevent illegal IP and MAC address binding, thus ensuring normal assignment of IP addresses by DHCP server.

Configuring DHCP

Configuring IP Pool

1. To configure or delete an IP pool, use the following command.

Step	Command	Function
1	`ZXR10(config)#`**ip pool** <*word*>	This creates IP pool which DHCP function uses and enters into IP pool of corresponding name configuration mode. **<***word***>** IP address pool name, 1~16 characters.
2	`ZXR10(config)#`**no ip pool** <*word*>	This deletes IP address pool which name corresponds.

2. To configure conflict time in ip pool or delete the orginal configuration, use the following commands.

Step	Command	Function
1	ZXR10(config-ip-pool)#**conflict-time** <*time*>	This configures conflict time in IP pool. <time> conflict time value, 1~18000 minutes, the default value is 30 minutes.
2	ZXR10(config-ip-pool)#**no conflict-time**	This deletes the original configuration and restores default time value.

3. To configure reserving address in IP pool or delete the original configuration, use the following commands.

Step	Command	Function
1	ZXR10(config-ip-pool)#**exclude** <*low_ip_addr*>[<*hig_ip_addr*>]	This configures reserving address in ip pool. <low_ip_addr >the begin low address of reserving address or a specific address. <Hig_ip_add r> the highest address of reserving address range. This command parameter must be a subset of this address pool.
2	ZXR10(config-ip-pool)#**no exclude** <*low_ip_addr*>[<*hig_ip_addr*>]	This deletes the original configuration. <low_ip_addr >the begin low address of reserving address or a specific address. <Hig_ip_add r> the highest address of reserving address range. This command parameter must be a subset of this address pool.

4. To add all suitable ip addresses to ip pool or delete the corresponding IP address range, use the following commands.

Step	Command	Function
1	ZXR10(config-ip-pool)#**network** <*net_number*><*net_mask*>	This adds all suitable IP addresses to IP pool. <net_numberr > a specific subnet network number, <net_maskr > subnet mask.
2	ZXR10(config-ip-pool)#**no network** <*net_number*><*net_mask*>	This deletes corresponding IP address range configuration. <net_numberr > a specific subnet network number, <net_maskr > subnet mask.

5. To configure IP pool range or delete corresponding IP address range , use the following commands.

Step	Command	Function
1	ZXR10(config-ip-pool)#**range** <*begin_ip_addr*><*last_ip_addr*><*ip_mask*>	This configures IP pool range. <begin_ip_addr > the beginning address of IP address pool, <last_n_ip_addr> the end address of IP address pool, <ip_mask r> mask.
2	ZXR10(config-ip-pool)#**no range** <*begin_ip_addr*><*last_ip_addr*><*ip_mask*>	This deletes corresponding IP address range configuration. <begin_ip_addr > the beginning address of IP address pool, <last_n_ip_addr> the end address of IP address pool, <ip_mask r> mask.

Configuring DHCP POOL

A DHCP pool will bind a ip pool. DHCP server will allocate address in binding address pool.

1. To configure a DHCP pool or delete a DHCP pool, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp pool** <*word*>	This configures a DHCP pool . <word> DHCP pool name
2	ZXR10(config)#**no ip dhcp pool** <*word*>	This deletes a DHCP pool.

2. To configure binding table between MAC address and ip address or delete the original configuration, use the following commands.

Step	Command	Function
1	ZXR10(config-dhcp-pool)#**binding** <*mac_addr*><*ip_addr*>[**vrf-instance** <*instance_ namer*>]	This configures binding table between MAC address and ip address. <mac_addr> Mac address <ip_addr> IP Address <instance_namer> instance name
2	ZXR10(config-dhcp-pool)#**no binding** <*mac_addr*><*ip_addr*>[**vrf-instance** <*instance_ namer*>]	This deletes the original configuration.

3. To configure a default route or delete the configured content, use the following commands.

Step	Command	Function
1	ZXR10(config-dhcp-pool)#**default-router** <*ip_addr*>[<*ip_addr*>][<*ip_addr*>]	This configures a default route.
2	ZXR10(config-dhcp-pool)#**no default-router** <*ip_addr*>[<*ip_addr*>][<*ip_addr*>]	This deletes the configured content.

4. To configure DNS server or delete the corresponding configuration, use the following commands.

Step	Command	Function
1	ZXR10(config-dhcp-pool)#**dns-server** <*ip_addr*>[<*ip_addr*>][<*ip_addr*>]	This configure DNS server address. This command can configure up to 8 DNS server addresses.
2	ZXR10(config-dhcp-pool)#**no dns-server** <*ip_addr*>[<*ip_addr*>][<*ip_addr*>]	This deletes the corresponding configuration.

5. To bind the specific ip pool with dhcp pool or delete binding relationship, use the following command.

Step	Command	Function
1	ZXR10(config-dhcp-pool)#**ip-pool** <*ip_pool_name*>	This binds the specific ip pool with dhcp pool. <ip_pool_namer> ip pool address pool name, 1~16 characters.
2	ZXR10(config-dhcp-pool)#**no ip-pool**	This deletes binding relationship.

6. To configure ip address lease-time or delete configured time, use the following commands.

Step	Command	Function
1	ZXR10(config)#**lease-time** [[**infinite**]|[<*days*><*hours*><*minutes*>]]	This configurse ip address lease-time. <days> 0~365 <hours> 0~23 <minutes> 0~59 infinite The default is 60 minutes.
2	ZXR10(config)#**no lease-time**	This deletes configured time.

7. To configure other options, use the following command.

Command	Function
ZXR10(config-dhcp-pool)#**option** <*option_code*>[[**ascii** <*string*>]|[**hex** <*hex_num*>]|[**ip** <*ip_addr*>]]	This configures other options. <option_code> configured optional code,1~254. <string> NVT ASCII character string. <hex_num> hexadecimal number. <ip_addr> IP Address

Configuring DHCP POLICY

1. To enter POLICY configuration mode or delete name corresponding policy configuration, use the following commands.

Step	Command	Function
1	ZXR10(config)#**ip dhcp policy** <*policy_name*><*priority*>	This enters policy configuration mode. <policy_namer> name of policy, 1~16 characters. <priority> priority.
2	ZXR10(config)#**no ip dhcp policy** <*policy_name*><*priority*>	This deletes name corresponding policy configuration.

2. To bind the policy to a dhcp-pool or delete binding relationship, use the following command.

Step	Command	Function
1	ZXR10(config-dhcp-pool)#**dhcp-pool** <*pool_name*>	This binds the policy to a dhcp-pool. <pool_name> name of dhcp pool
2	ZXR10(config-dhcp-pool)#**no dhcp-pool** <*pool_name*>	This deletes binding relationship.

3. To configure relay agent address or delete the configuration, use the following commands.

Step	Command	Function
1	ZXR10(config-dhcp-pool)#**relay-agent** <*ip_addr*>	This configures relay agent address. <ip_addr> IP Address
2	ZXR10(config-dhcp-pool)#**no relay-agent**	This deletes configuration.

Configuring DCHP Server

1. To enable DHCP or stop DHCP, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp enable**	After enabling DHCP, system will take DHCP ip address request on the interface which is configured user interface attribute. This system builts in DHCP Server function and DHCP Relay function which are enabled by using this command. By default, disable DHCP.
2	ZXR10(config)#**no ip dhcp enable**	This stops DHCP.

2. To enable DHCP working mode on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**ip dhcp mode** [**server** | **relay** | **proxy**]	Relay: enalbe DHCP Relay on the interface; server: enable DHCP Server on the interface; proxy:enable DHCP Proxy on the interface.

After enabling built-in DHCP Relay process, system processes IP address request sent from DHCP client on the interface and allocate IP address for DHCP Client dynamically by external DHCP Server configured in the interface.

After enabling built-in DHCP Proxy process, system will process IP address request sent from DHCP client on the interface, allocate IP address for DHCP Client dynamically by external DHCP Server configured in the interface and replace the long lease with short lease to client. When DHCP Client sending continue-to-rent request, if the long lease allocated by DHCP Server is not timeout, DHCP Proxy will response DHCP Client directly and won't send continue-to-rent request to external DHCP Server to relieve the burden of external DHCP Server.

Only one function among system built-in DHCP Server function, DHCP Relay function and DHCP Proxy function can be run on the same interface.

3. To bind policy to an interface or delete configuration, use the following commands.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp policy** < *policy_name*>	This binds policy to an interface. <policy_name> the policy name that interface need bind.
2	ZXR10(config-if-vlanX)#**no ip dhcp policy**	This deletes configuration.

4. To configure DHCP user quota on interface or cancel this configuration, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp user quota** <*limit-value*>	This configures DHCP user quota on interface, that is , the maximum number of DHCP Client on the interface. <limit-value> DHCP user quota1~2048. The default: no quota.
2	ZXR10(config-if-vlanX)#**no ip dhcp user quotar**	This cancel dhcp user quota.

As for DHCP Server, DHCP user quota is used to limit the max number of DHCP users on an interface, thus limiting the number of IP addresses assigned on the interface.

As for DHCP Relay, DHCP Relay standard mode doesn't support DHCP user quota, thus user quota doesn't take effect. But if DHCP Relay is configured forwarding in safety mode, DHCP Relay will make DHCP user quota configuration valid.

5. To configure the interface select outside DHCP Server policy or cancel this policy, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp helper-address policy vclass-id**	This configures the interface select outside DHCP Server policy. The default is to select DHCP Server in ip dhcp relay server command on the interface.
2	ZXR10(config-if-vlanX)#**no ip dhcp helper-address policy vclass-id**	This cancels this interface select outside DHCP Server policy.

6. To configure DHCP SERVER/RELAY/PROXY ramble function or disable DHCP ramble function, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp ramble**	When DHCP ramble function is enabled, DHCP user can switch the access interface on-line. The default: disable DHCP ramble function.
2	ZXR10(config)#**no ip dhcp ramble**	This disables DHCP ramble function.

7. To enable DHCP log print switch or stop DHCP print function, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp logging on**	This enables DHCP log print switch. The default is to disable DHCP log print function. After DHCP log print function is enabled, DHCP user on-line log will be recorded.
2	ZXR10(config)#**no ip dhcp logging on**	This disables DHCP print function.

Configuring DHCP Snooping

1. To add the binding entry to binding-database manually or delete binding entry from DHCP SNOOPING binding-database, use the following commands.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping binding** <*mac*> **vlan** <*vlan*><*ip address*><*interface-number*> **expiry** <*2147483647*>	This adds user binding entry to binding-database manually. <mac> user MAC address <vlan> the VLAN user belongs to, 1~4096input the range. <ip address> DHCP binding IP address. <interface-number> physical interface numbersuch as fei, gei and smartgroup.
2	ZXR10(config)#**no ip dhcp snooping binding** <*mac*> **vlan** <*vlan*><*ip address*><*interface-number*>	This deletes user binding entry from DHCP SNOOPING binding database.

2. To delete the entry of DHCP SNOOPING binding table on layer 2 interface manually, use the following command.

Command	Function
ZXR10(config)#**ip dhcp snooping clear** [<*interface-number*>]	This deletes the entry of DHCP SNOOPING binding table on layer 2 interface manually. <interface-number> physical interface numbersuch as fei, gei and smartgroup.

3. To enable DHCP SNOOPING or disable DHCP SNOOPING, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping enable**	After DHCP SNOOPING is globally enabled, DHCP SNOOPING need to be enabled on the corresponding VLAN to take effect on it.
2	ZXR10(config)#**no ip dhcp snooping enable**	This disables DHCP SNOOPING function.

4. To configure if 82 option is inserted when DHCP SNOOPING is configured, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping information option**	This inserts 82 option.
2	ZXR10(config)#**no ip dhcp snooping information option**	This doesn't insert 82 option.

5. To configure the 82 option format or delete the configured 82 option format and restore the default format, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping information format** {**china-tel** | **dsl-forum**}	This configures 82 option format which is inserted when DHCP SNOOPING is configured, china-tel: China Telecom 82 option format. dsl-forum:DSL forum 82 option format. The default is China Telecom 82 option format.
2	ZXR10(config)#**no ip dhcp snooping information format**	This cancels configured 82 option format to restore default format.

6. To configure the policy of forwarding DHCP data packet 82 option or cancel the policy, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping information policy** {**keep** | **replace**}	This configures the policy of forwarding DHCP data packet 82 option. keep: keep the original 82 option and transparently transmit. replace: replace the original 82 option. The default is to keep the original 82 option and transparently transmit.
2	ZXR10(config)#**no ip dhcp snooping information policy**	This cancels configured 82 option policy to restore default format.

7. To configure DHCP SNOOPING ramble function and allow user to switch on different ports, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping ramble**	This configures DHCP SNOOPING ramble function.
2	ZXR10(config)#**no ip dhcp snooping ramble**	This disables DHCP SNOOPING ramble function.

8. To configure the interface connects to DHCP SERVER as trust interface, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping trust** <*interface-number*>	This configures DHCP SERVER interface as trust interface. <interface-number> physical interface numbersuch as fei, gei and smartgroup.
2	ZXR10(config)#**no ip dhcp snooping trust** <*interface-numbe*>	This cancels DHCP SERVER interface as trust interface.

9. To enable DHCP SNOOPING on the specific VLAN, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp snooping vlan** <*vlan*>	This enables DHCP SNOOPING on the specific VLAN. <vlan> the VLAN user belongs to, 1~4094input the range.
2	ZXR10(config)#**no ip dhcp snooping vlan** <*vlan*>	This cancels DHCP SNOOPING on the specific VLAN.

Configuring DHCP Relay

1. To configure the DHCP agent ip address on the interface or delete the ip address, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp relay agent** <*ip-address*>	This configures the DHCP agent ip address on the interface. < ip-address> DHCP agent IP address on the interface, in dotted decimal notation.
2	ZXR10(config-if-vlanX)#**no ip dhcp relay agent**	This deletes the DHCP agent ip address on the interface.

Before enabling DHCP Relay to forward user DHCP request to external DHCP Server, it is needed to configure IP address of DHCP Agent, which is one of the IP addresses of interfaces where DHCP Client locates.

External DHCP Server will assign IP address according to IP address of DHCP Agent to make them in the same subnet. DHCP reply packet returned to DHCP client by DHCP server is forwarded by DHCP Agent. Therefore, a route pointing to the subnet where DHCP Agent locates needs to be configured on external DHCP Server.

2. To configure the outside DHCP server ip address on the interface or delete outside DHCP Server address on the interface, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp relay server** <*ip-address*>{**standard** | **security**}	<ip-address>outside DHCP Server ip address, in dotted decimal notation standard: comply with DHCP standard protocol forwarding mode security: ZTE security forwarding mode, The default is standard.
2	ZXR10(config-if-vlanX)#**no ip dhcp relay server** <*ip-address*>	<ip-address>outside DHCP Server ip address, in dotted decimal notation

Standard forwarding mode conforms to DHCP standard protocol. After user obtains corresponding IP address, DHCP process will not process subsequent unicast interaction any more, such as security inspection. At the same time, writing ARP table function is invalid for standard mode. Standard forwarding mode performance will be better for big consumer number because it does not deal with the subsequent unicast interaction.

Security forwarding mode combines DHCP standard protocol with ZTE patent technology to control and manage all interaction of DHCP client and outside DHCP SERVER such as security check. Therefore, DHCP process can work in all DHCP interaction. At the same time, it supports ARP writing function. System default Relay forwarding mode is standard forwarding mode.

3. To configure the retry time that DHCP Relay applies from outside DHCP Server or recover default retry time, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay server retry** <*limit-values*>	<limit-value> the retry time that DHCP Relay applies from outside DHCP Server. The range is 5~1000. The value is 10 by default.
2	ZXR10(config)#**no ip dhcp relay server retry**	This recovers default retry time.

4. To configure the specific domain name DHCP CLient applies from outside DHCP Server, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay server vclass-id** <*domain name*><*ip-address*>{**standard** | **security**}	<domain name> domain name that DHCP Client request packet carries. <ip-address>outside DHCP Server ip address, in dotted decimal notation standard: comply with DHCP standard protocol forwarding mode security: ZTE security forwarding mode.
2	ZXR10(config)#**no ip dhcp relay server vclass-id** <*domain name*><*ip-address*>	<domain name> domain name that DHCP Client request packet carries. <ip-address>outside DHCP Server ip address, in dotted decimal notation

5. To configure unrestricted DHCP user message on DHCP Relay standard mode or restrict DHCP user message, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay forward reply unrestricted**	This configurse unrestricted DHCP user message on DHCP Relay standard mode.
2	ZXR10(config)#**no ip dhcp relay forward reply unrestricted**	This restricts DHCP user message and recovers default mode.

DHCP client continuous rent is launched by DHCP client. For that DHCP client does not send continuous rent message, if can receive ACK message that DHCP Server response to client, it is taken for granted that DHCP client is on-line and send transparently this message to client.

6. To configure the insert 82 option when the DHCP process is in relay forwarding or cancel the insert of 82 option, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay information option**	This configures the insert 82 option when the DHCP process is in relay forwarding. The default: 82 option is not inserted.
2	ZXR10(config)#**no ip dhcp relay information option**	This cancels the insert 82 option.

7. To configure the DHCP process when the insert 82 option has been configured in the DHCP process in relay forwarding data and host should configure the insert 82 option or delete configured 82 option handle policy, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay information policy** {**keep** | **replace**}	keep: keep the original 82 option and transparently transmit. replace: replace the original 82 option. The default is to keep the original 82 option and transparently transmit.
2	ZXR10(config)#**no ip dhcp relay information policy**	This cancels configured 82 option policy to restore default policy.

8. To configure DHCP client server-id that DHCP Relay responses or cancel DHCP client server-id that DHCP Relay responses, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay security client server-id** <*ip-address*>	This configures DHCP client server-id that DHCP Relay response. <ip-address> server-id ip addressin dotted decimal notation.
2	ZXR10(config)#**no ip dhcp relay security client server-id**	This cancels DHCP client server-id that DHCP Relay responses.

9. To enable DHCP Relay Snooping, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay snooping enable**	This enables DHCP Relay Snooping. DHCP Relay Snooping is disabled by default.
2	ZXR10(config)#**no ip dhcp relay snooping enable**	This cancels DHCP Relay Snooping function.

10. To enable DHCP network packet that all reply on the interface, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp relay snooping packet reply**	This enables DHCP network packet that all reply on the interface.
2	ZXR10(config-if-vlanX)#**no ip dhcp relay snooping packet reply**	This command disables DHCP network packet that all reply on the interface.

11. To enable DHCP network packet that all request on the interface, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp relay snooping packet request**	This enables DHCP network packet that all request on the interface.
2	ZXR10(config-if-vlanX)#**no ip dhcp relay snooping packet request**	This disables DHCP network packet that all request on the interface.

12. To enable the interface as DHCP Relay trust or disable the interface as DHCP Relay trust, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp relay snooping trust**	This enables the interface as DHCP Relay trust.
2	ZXR10(config-if-vlanX)#**no ip dhcp relay snooping trust**	This disables the interface as DHCP Relay trust.

13. To enable DHCP Relay Snooping Trust or disable DHCP Relay Snooping Trust, use the following command.

Step	Command	Function
1	ZXR10(config)#**ip dhcp relay snooping trust enable**	This enables DHCP Relay Snooping Trust.
2	ZXR10(config)#**no ip dhcp relay snooping trust enable**	This disables DHCP Relay Snooping function.

Configuring DHCP Client

1. To enable class-id of dhcp client on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**ip dhcp client class-id** {**WORD** | **hex**}	This enables class-id of dhcp client on the interface.

2. This configures class-id of dhcp client on the interface.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp client client-id**	This configures dhcp client-id on the interface.
2	ZXR10(config-if-vlanX)#**no ip dhcp client client-id**	This cancels the configuration of dhcp client-id on the interface.

3. To configure hostname of dhcp client on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**ip dhcp client hostname WORD**	This configures hostname of dhcp client on the interface.

4. To configure lease information of dhcp client on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**ip dhcp client lease** { **0-365** | **infinite** }	This configures lease information of dhcp client on the interface.

5. To configure request information of dhcp client on the interface, use the following command.

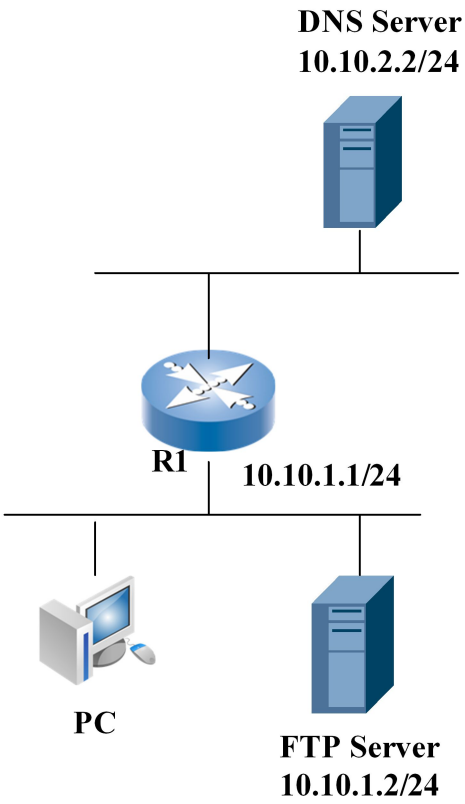
Command	Function
ZXR10(config-if-vlanX)#**ip dhcp client request** { **dns-nameserver** | **domain-name** | **router** | **static-route** | **tftp-server-address** }	This configures request information of dhcp client on the interface.

DHCP Configuration Example

DHCP Server Configuration Example

R1 acts as the DHCP server and default gateway and the host obtains IP addresses through the DHCP dynamically, as shown in Figure 22.

FIGURE 22 DHCP SERVER CONFIGURATION



R1 configuration:

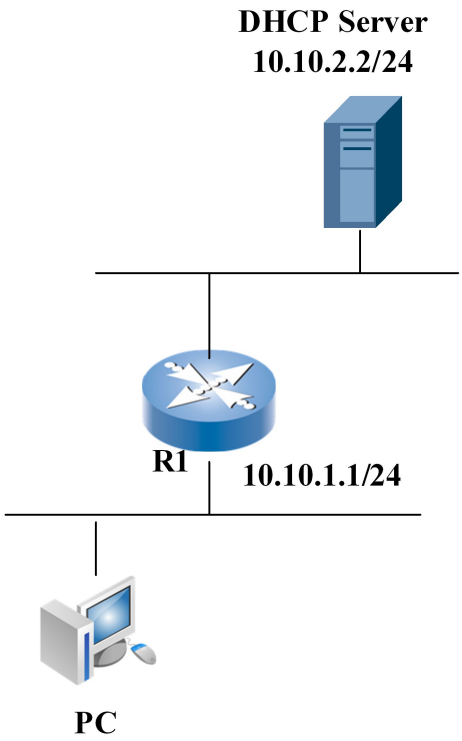
```
ZXR10(config)#interface vlan 10
ZXR10(config-if-vlan10)#ip dhcp mode server
ZXR10(config-if-vlan10)#ip address 10.10.1.1 255.255.255.0
ZXR10(config-if-vlan10)#exit
ZXR10(config)#ip pool pool1
ZXR10(config-ip-pool)#range 10.10.1.10 10.10.1.100 255.255.255.0
ZXR10(config-ip-pool)#exit
ZXR10(config)#ip dhcp pool dhcp1
ZXR10(config-dhcp-pool)#ip-pool pool1
ZXR10(config-dhcp-pool)#exit
ZXR10(config)#ip dhcp policy p1 1
ZXR10(config-dhcp-policy)#dhcp-pool dhcp1
ZXR10(config-dhcp-policy)#default-route 10.10.1.1
ZXR10(config-dhcp-policy)#exit
ZXR10(config)#interface vlan 10
ZXR10(config-if-vlan10)#ip dhcp policy p1
ZXR10(config)#ip dhcp enable
```

DHCP Relay Configuration Example

Router at the user end is connected directly as DHCP relay when the DHCP client and server are not in the same network.

R1 enables DHCP relay function and a single server 10.10.2.2 provides DHCP server function. This mode is usually adopted when a lot of hosts require the DHCP service. This is shown in Figure 23.

FIGURE 23 DHCP RELAY CONFIGURATION



R1 configuration:

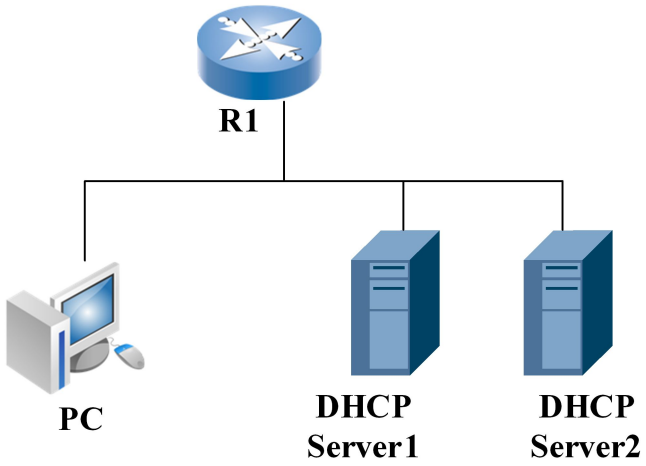
```
ZXR10(config)#interface vlan10
ZXR10(config-if-vlan10)#ip dhcp mode relay
ZXR10(config-if-vlan10)#ip address 10.10.1.1 255.255.255.0
ZXR10(config-if-vlan10)#ip dhcp relay agent 10.10.1.1
ZXR10(config-if-vlan10)#ip dhcp relay server 10.10.2.2
ZXR10(config-if-vlan10)#exit
ZXR10(config)#ip dhcp enable
```

DHCP Snooping Configuration Example

DHCP server 1 connects to the interface gei_1/1 in switch R1. Manager configures the DHCP. The server 2 connects to the interface gei_1/2 in switch R1. This is configured by the user, it is illegal DHCP server. Both ports gei_1/1 and gei_1/2 are in vlan 100. Enable the DHCP snooping function in the switch can prevent set illusive DHCP server.

Now it is needed to enable DHCP Snooping function in vlan 100 and configure the interface gei_1/1 be trust interface. This is shown in Figure 24.

FIGURE 24 DHCP SNOOPING CONFIGURATION



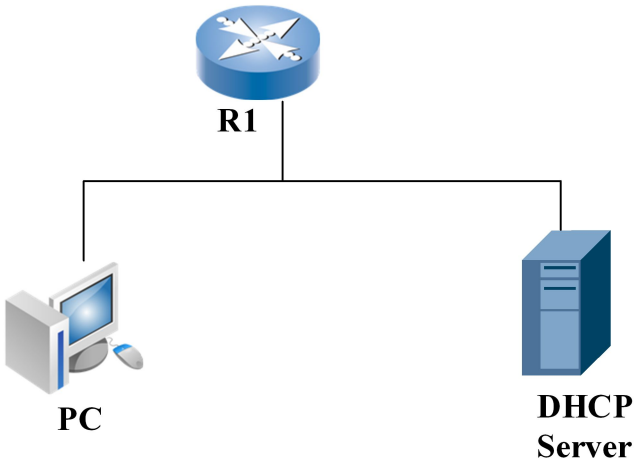
R1 configuration:

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#switch access vlan 100
ZXR10(config-gei_1/1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#switch access vlan 100
ZXR10(config-gei_1/2)#exit
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#ip dhcp snooping trust gei_1/1
```

DHCP Snooping Prevent Static IP Configuration Example

DHCP server belongs to vlan 100 and PC belongs to vlan 200. PC gets the IP address use by DHCP. Now it is required to forbid the PC to configure the static IP address through the DHCP snooping and dynamic ARP inspection technologies. This illustration is shown in Figure 25.

FIGURE 25 DHCP SNOOPING PREVENT STATIC IP CONFIGURATION



R1 configuration:

```
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#vlan 100
ZXR10(config-vlan100)#ip arp inspection
```

DHCP Maintenance and Diagnosis

1. To display configuration information of the DHCP relay process module, use the following command.

   show ip dhcp relay [**forward** | **information** | **security** | **server** | **snooping** | **user**]

2. To display configuration information of the local address pool, use the following command.

   show ip local pool [<*pool-name*>]

3. To display configuration information of interface-related DHCP server/relay, use the following command.

   show ip interface

4. To display the DHCP snooping configuration, use the following command.

   show ip dhcp snooping configure

5. To view the DHCP snooping Vlan, use the following command.

   show ip dhcp snooping vlan [<*vlan-id*>]

6. To view the IP DHCP snooping trust, use the following command.

   show ip dhcp snooping trust

7. To display DHCP snooping database, use the following command.

   show ip dhcp snooping database <*port-number*>

8. To view dynamic arp inspection, use the following command.

   show ip arp inspection vlan [<*vlanl-id*>]

9. To display DHCP pool, use the following command.

   show ip dhcp pool [<*pool-name*>]

10. To display DHCP policy, use the following command.

    show ip dhcp policy [<*policy_name*>]

To handle DHCP server/relay processes, use **debug ip dhcp**command.

Chapter 10

VRRP Configuration

Table of Contents

VRRP Overview

Host in a broadcast domain usually sets a default gateway as the next hop of route packets. The host in the broadcast domain cannot communicate with the host in another network unless the default gateway works normally. To avoid the single point of failure caused by the default gateway, multiple router interfaces are configured in the broadcast domain and run the Virtual Router Redundancy Protocol (VRRP) in these routers.

VRRP is used to configure multiple router interfaces in a broadcast domain into a group to form a virtual router and assigns an IP address to the router to function as its interface address. This interface address may be the address of one of router interfaces or the third party address.

The router is used as the master router if its interface address is used and other routers are used as the backup ones. The router with high priority is used as the master router if the third party address is used. If two routers have the same priority, the one with the greater interface address wins. For ZXR10 5900/5200, if the two routers priorities are same, master apply priority rule.

Set the IP address of the virtual router to gateway on the host in this broadcast domain. The master router is replaced with the backup router with the highest priority if the master router is faulty, without affecting the host in this domain. The host in this domain cannot communicate with outside world only when all routers in the VRRP group work abnormally.

These routers can be configured into multiple groups for mutual backup. The hosts in the domain use different IP addresses as gateway to implement data load balance.

Configuring VRRP

1. To run VRRP, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **ip** <*ip-address*>[**secondary**]	This runs VRRP.

This configures multiple virtual addresses in a VRRP group and the linked host can use any address as gateway for communication.

2. To configure VRRP priority on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **prirority** <*priority*>	This configures VRRP priority on the interface.

3. To configure whether preemption is enabled on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **preempt** [**delay** <*milliseconds*>]	To configure whether preemption is enabled on the interface, use the following command.

4. To configure the time interval for sending VRRP notifications on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **advertise** [**msec**]<*interval*>	This configures the time interval for sending VRRP notifications on the interface.

5. To configure how to learn about the time interval for sending VRRP packets on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **learn**	This configures how to learn about the time interval for sending VRRP packets on the interface.

6. To configure authentication character string on the interface, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **authentication** <*string*>	This configures authentication character string on the interface.

7. To configure VRRP up-flow link track function, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** <*group*> **track** <*track-num*>[**decrement**<*priority*>]	This configures VRRP up-flow link track function.

8. To configure the mode of virtual device, use the following command.

Command	Function
ZXR10(config-if-vlanX)#**vrrp** < *group*> **mode** {**private** | **standard**}	This configures the mode of virtual device

9. To configure virtual device vrrp protocol message out-interface, use the following command.

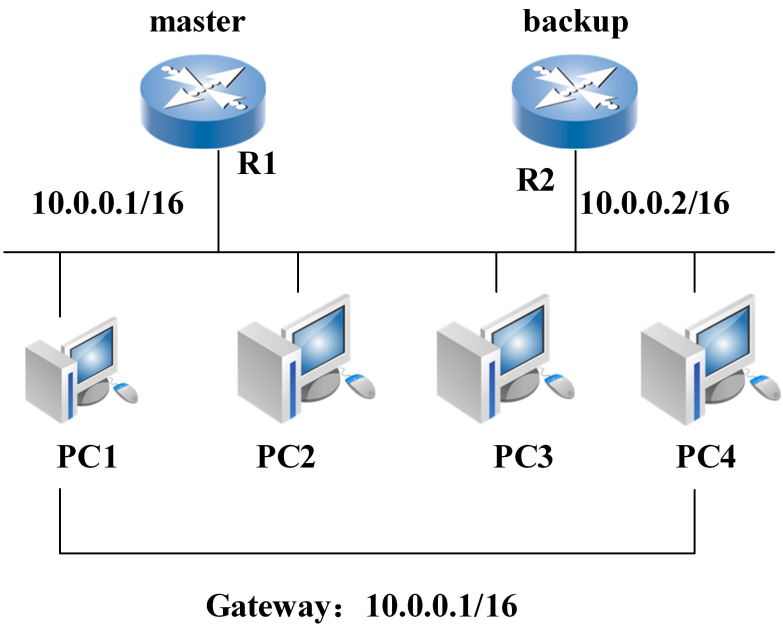
Command	Function
ZXR10(config-if-vlanX)#**vrrp** < *group*> **out-interface** <*interfacename*>	This configures virtual device vrrp protocol message out-interface.

VRRP Configuration Example

Basic VRRP Configuration Example

This example shows that R1 and R2 run in the VRRP protocol between each other. R1 interface address 10.0.0.1 is used as the VRRP virtual address, therefore R1 is considered as a master router. This is shown in Figure 26.

FIGURE 26 BASIC VRRP CONFIGURATION



R1 configuration:

```
ZXR10_R1(config)#interface vlan 1
ZXR10_R1(config-if-vlan1)#ip address 10.0.0.1 255.255.0.0
ZXR10_R1(config-if-vlan1)#vrrp 1 ip 10.0.0.1
```

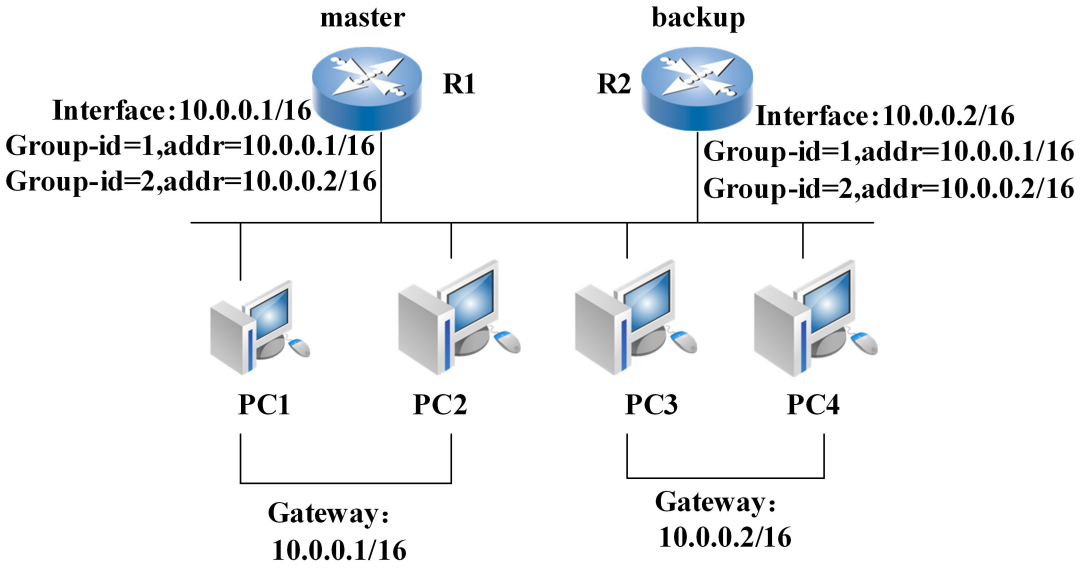
R2 configuration:

```
ZXR10_R2(config)#interface vlan 1
ZXR10_R2(config-if-vlan1)#ip address 10.0.0.2 255.255.0.0
ZXR10_R2(config-if-vlan1)#vrrp 1 ip 10.0.0.1
```

Symmetric VRRP Configuration Example

Two VRRP groups are booted in this example, where PC1 and PC2 use the virtual router in Group 1 as default gateway with the address 10.0.0.1. PC3 and PC4 use the virtual router in Group 2 as default gateway with the address 10.0.0.2. R1 and R2 serve as mutual backup. Four hosts cannot communicate with outside world until both routers become invalid. This is shown in Figure 27.

FIGURE 27 SYMMETRIC VRRP CONFIGURATION



R1 configuration:

```
ZXR10_R1(config)#interface vlan 1
ZXR10_R1(config-if-vlan1)#ip address 10.0.0.1 255.255.0.0
ZXR10_R1(config-if-vlan1)#vrrp 1 ip 10.0.0.1
ZXR10_R1(config-if-vlan1)#vrrp 2 ip 10.0.0.2
```

R2 configuration:

```
ZXR10_R2(config)#interface vlan 1
ZXR10_R2(config-if-vlan1)#ip address 10.0.0.2 255.255.0.0
ZXR10_R2(config-if-vlan1)#vrrp 1 ip 10.0.0.1
ZXR10_R2(config-if-vlan1)#vrrp 2 ip 10.0.0.2
```

VRRP Maintenance and Diagnosis

To perform VRRP maintenance and diagnosis, ZXR10 5900/5200 provides the following commands to view all VRRP configuration information.

show vrrp [<*group*>|**brief**|**interface** <*interface-name*>|**all**]

ZXR10 5900/5200 provides **debug vrrp** command to display VRRP debug information switch.

debug vrrp {**state**|**packet**|**event**|**error**|**all**}

This page is intentionally blank.

Chapter 11

Network Management Configuration

Table of Contents

NTP Configuration

NTP Overview

Network Time Protocol (NTP) is the protocol used to synchronize the clocks of computers on a network or across multiple networks, like the Internet. Without adequate NTP synchronization, organizations cannot expect their network and applications to function properly. In practice, ZXR10 5900/5200 can act as the NTP client and support the configuration of at most 5 NTP time servers.

Configuring NTP

1. To define a time server, use the following command.

Command	Function
ZXR10(config)#**rmon collection statistics** <*index*>[**owner** <*string*>]	This defines a time server. Priority must be selected. Each server priority is different and the range is 1~5; Version is option , the range is 1~3 , the default is 3. Key is valid when authentication is enabled and option; Lock/unlock is used to configure if server is locked and option.

2. To enable NTP function, use the following command.

Command	Function
ZXR10(config)#**ntp enable**	This enables NTP function.

3. To configure the source address used by the NTP in the process of sending a synchronization time request, use the following command.

Command	Function
ZXR10(config)#**ntp source** <*ip-address*>	This configures the source address used by the NTP in the process of sending a synchronization time request.

4. To configure time zone of the switch, use the following command.

Command	Function
ZXR10(config)#**clock timezone**	This configures time zone of the switch.

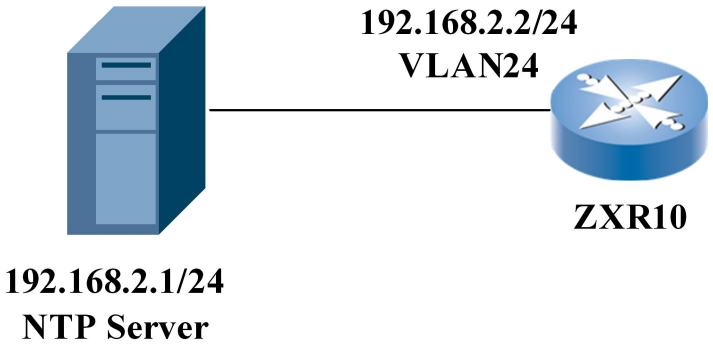
5. To view the NTP running state, use the following command.

Command	Function
ZXR10(config-router)#**show ntp status**	This views the NTP running state.

NTP Configuration Example

This example shows routing switch as a NTP client and assume that the NTP protocol version is 2. This is shown in Figure 28.

FIGURE 28 NTP CONFIGURATION EXAMPLE



ZXR10 Configuration:

```
ZXR10(config)#interface vlan24
ZXR10(config-if-vlan24)#ip address 192.168.2.2 255.255.255.0
ZXR10(config-if-vlan24)#exit
ZXR10(config)#ntp enable
ZXR10(config)#ntp server 192.168.2.1 version 2
```

RADIUS Configuration

RADIUS Overview

Remote Authentication Dial In User Service (RADIUS) is a standard AAA protocol. AAA represents Authorization, Authentication and Accounting. AAA is used to authenticate the users accessing the routing switch and prevent illegal users from accessing which results in enhancing security of the equipment.

ZXR10 5900/5200 supports RADIUS authentication function to authenticate Telnet users accessing the routing switch.

ZXR10 5900/5200 supports multiple RADIUS server groups. Three authentication servers can be configured in each RADIUS group. The server timeout time and times of timeout retransmission can be set for each group. The administrator can configure different RADIUS groups to select a specific RADIUS server.

Configuring RADIUS

1. To configure RADIUS accounting group, use the following command.

Command	Function
ZXR10(config)#**radius accounting-group** <*group-number*>	This configures RADIUS accounting group.

2. To configure RADIUS authentication group, use the following command.

Command	Function
ZXR10(config)#**radius authentication-group** <*group-number*>	This configures RADIUS authentication group.

3. To configure the parameters of RADIUS, peform the following steps.

Step	Command	Function
1	ZXR10(config-authgrp-1)#**timeout** <*timeout*>	This configures timeout retry parameter of RADIUS server.
2	ZXR10(config-authgrp-1)#**algorithm** {**first**|**round-robin**}	This configures algorithm of RADIUS server.
3	ZXR10(config-authgrp-1)#**alias** <*name-str*>	This configures alias of RADIUS server group.
4	ZXR10(config-authgrp-1)#**calling-station-format** < *Format number*>	This configures format of command calling-station-id.
5	ZXR10(config-authgrp-1)#**deadtime** <*time*>	This configures dead time of authentication server.
6	ZXR10(config-authgrp-1)#**max-retries** <*times*>	This configures timeout retry parameter of RADIUS server.
7	ZXR10(config-authgrp-1)#**nas-ip-address** < *NAS IP address*>	This configures nas-ip of RADIUS server, which corresponds to nas-ip and source ip address of protocol packets.
8	ZXR10(config-authgrp-1)#**server** <*ipaddress*> **key** <*keystr*> **port** <*portnum*>	This configures radius server and its parameter.
9	ZXR10(config-authgrp-1)#**user-name-format** {**include-domain**|**strip-domain**}	This configures format of user name which BRAS sends to RADIUS server.
10	ZXR10(config-authgrp-1)#**vendor** {**enable**|**disable**}	This configures whether self-definition attribute of manufacturer is in a sending RADIUS protocol packet.

4. To perform RADIUS maintenance and diagnosis, execute the following commands.

Command	Function
ZXR10#**debug radius** {**accounting** {**event**| **error**|**data** | **packet** <*group-number*|**all**>}| **authentication** {**event**| **error**|**data** | **packet** <*group-number*|**all**>}|**user user-nam**|**all**|**exception**}	This displays RADIUS debugging information.
ZXR10#**show counter radius** {**accounting-group group-number** | **authentication-group group-number**|**all**}	This displays statistics information.
ZXR10#**show accounting local-buffer** {**group group-number**|**name radiusname**|**session session-id**|**user user-name**|**sum**|**all**}	This displays the content of accounting packets in local buffer.
ZXR10#**clear accounting local-buffer** [**group number** | **all**]	This clears the content of accounting packets in local buffer.

RADIUS Configuration Example

The mode of configuring accounting group is same as that of configuring authentication group. The following example is how to configure accounting group.

```
ZXR10(config)#radius accounting-group 1
ZXR10(config-acct-group-1)#algorithm round-robin
ZXR10(config-acct-group-1)#calling-station-format 2
ZXR10(config-acct-group-1)#deadtime 5
ZXR10(config-acct-group-1)#local-buffer enable
ZXR10(config-acct-group-1)#max-retries 5
ZXR10(config-acct-group-1)#nas-ip-address 10.1.1.4
ZXR10(config-acct-group-1)#server 1 10.2.1.3 key uas
ZXR10(config-acct-group-1)#server 2 12.1.2.3 key uas
ZXR10(config-acct-group-1)#timeout 10
```

SNMP Configuration

SNMP Overview

Simple Network Management Protocol (SNMP) is the most popular NMS protocol nowadays. An NMS server can manage all the devices on the network through this protocol.

SNMP is managed based on server and client. The background NMS server serves as the SNMP server and the foreground network device serves as SNMP client. The foreground and background share an MIB and communicate with each other through the SNMP protocol. It is required to configure the specific SNMP server for the rouging switch as the SNMP agent and define contents and authorities availably collected by the NMS. ZXR10 5900/5200 supports multiple versions of SNMP.

Configuring SNMP

1. To set the SNMP packet community, use the following command.

Command	Function
ZXR10(config)#**snmp-server community** <*community-name*>[**view** <*view-name*>][**ro**|**rw**]	This sets the SNMP packet community.

SNMPv1/v2c adopts the community authentication mode. SNMP community is named by character strings and different communities have read-only or read-write access authorities. Community with read-only authority can only query equipment information. and the community with read-write authority can configure the equipment.

Both read-only and read-write are limited by the view. Operations can only be conducted in the permitted view range. If parameter view is omitted use default view and use parameter ro if ro/rw are omitted.

2. To define a SNMPv2 view, use the following command.

Command	Function
ZXR10(config)#**snmp-server view** <*view-name*><*subtree-id*>{**included**|**excluded**}	This defines a SNMPv2 view.

3. To set the system handler contract mode (SysContact) of the MIB object, use the following command.

Command	Function
ZXR10(config)#**snmp-server contact** <*mib-syscontact-text*>	This sets the system handler contract mode (SysContact) of the MIB object.

SysContact is a management variable of the system group in the MIB II and it records ID and contact mode of the relevant personnel of the managed equipment.

4. To set the location (SysLocation) of the MIB object, use the following command.

Command	Function
ZXR10(config)#**snmp-server location** <*mib-syslocation-text*>	This sets the location (SysLocation) of the MIB object.

SysLocation is a management variable of the system group in the MIB II and is used to indicate the location of the managed equipment.

5. To set the types of TRAP allowed for sending, use the following command.

Command	Function
ZXR10(config)#**snmp-server enable trap** [<*notification-type*>]	This sets the types of TRAP allowed for sending.

TRAP is un-requested information sent by the managed equipment initiatively to the NMS and is used to report some emergent events.

6. To set the TRAP destination host, use the following command.

Command	Function
ZXR10(config)#**snmp-server host** [**mng**]<*ip-address*>[**trap**|**inform**][**version** {**1**|**2c**|**3** {**auth**|**noauth**|**priv**}}]<*community-name*>[**udp-port** <*udp-port*>][**...**<*trap-type*>]	This sets the TRAP destination host.

ZXR10 5900/5200 supports five kinds of ordinary traps: SNMP, bgp, OSPF, RMON and stalarm.

7. To use ACL to control the host that can access the switches through SNMP protocol, use the following command.

Command	Function
ZXR10(config)#**snmp-server access-list** <*acl-number*>	This uses ACL to control the host that can access the switches through SNMP protocol.

8. To define context name of SNMP, use the following command.

Command	Function
ZXR10(config)#**snmp-server context** < *context name* >	This defines context name of SNMP.

9. To set local engine id of SNMPv3, use the following command.

Command	Function
ZXR10(config)#**snmp-server engine-id** <*engine-id*>	This sets local engine id of SNMPv3.

10. To configure safe mode group of user, use the following command.

Command	Function
ZXR10(config)#**snmp-server group** <*groupname*> **v3** {**auth**|**noauth**|**priv**}[**context** <*context-name*> **match-prefix**|**match-exact**][**read** <*readview*>][**write** <*writeview*>][**notify** <*notifyview*>]	This configures safe mode group of user.

11. To set the maximum packet size of SNMP, use the following command.

Command	Function
ZXR10(config)#**snmp-server packetsize** <*484-1400*>	This sest the maximum packet size of SNMP.

12. To configure TRAP source, use the following command.

Command	Function
ZXR10(config)#**snmp-server trap-source** <*IP address*>	This configures TRAP source.

13. To configure the users which are allowed to access SNMP engine, use the following command.

Command	Function
ZXR10(config)#**snmp-server user** <*username*><*groupname*> **v3** [**encrypted**][**auth** {**md5**|**sha**}<*auth-password*>[**priv des56** <*priv-password*>]]	This configures the users which are allowed to access SNMP engine.

14. To display relevant information of SNMP, use the following command.

Command	Function
ZXR10(config)#**show snmp**	This displays relevant information of SNMP.

15. To display configuration information of SNMP, use the following command.

Command	Function
ZXR10(config)#**show snmp config**	This displays configuration information of SNMP.

16. To display users of SNMPv3, use the following command.

Command	Function
ZXR10(config)#**show snmp user**	This displays users of SNMPv3.

17. To display information of SNMPv3 group, use the following command.

Command	Function
ZXR10(config)#**show snmp group**	This displays information of SNMPv3 group.

18. To display SNMP engine ID, use the following command.

Command	Function
ZXR10(config)#**show engine-id**	This displays SNMP engine ID.

SNMP Configuration Example

The following is an example of SNMP configuration.

```
ZXR10(config)#snmp-server view myViewName 1.3.6.1.2.1 included
ZXR10(config)#snmp-server community myCommunity view myview rw
ZXR10(config)#snmp host 168.1.1.1 trap ver 1 ospf
ZXR10(config)#snmp-server location  this is ZXR10 in china
ZXR10(config)#snmp-server contact this is ZXR10, tel: (025)2872006
```

RMON Configuration

RMON Overview

Remote Monitoring (RMON) system is to monitor network terminal services. A remote detector, the local routing switch system, completes data collection and processing through the RMON. The routing switch contains RMON agent software communicating with the NMS through the SNMP. Information is usually transmitted from the routing switch to the NMS.

Configuring RMON

1. To enable the interface statistics function (only for Ethernet), use the following command.

Command	Function
ZXR10(config-gei_1/x)#**rmon collection statistics** <*index*>[**owner** <*string*>]	This enables the interface statistics function (only for Ethernet) .

2. To set an alarm and MIB object, use the following command.

Command	Function
ZXR10(config)#**rmon alarm** <*index*><*variable*><*interval*>{**delta**|**absolute**} **rising-thershold** <*value*>[<*event-index*>] **falling-threshold** <*value*>[<*event-index*>][**owner** <*string*>]	This sets an alarm and MIB object.

3. To enable the history collection function of the interface, use the following command.

Command	Function
ZXR10(config-gei_1/x)#**rmon collection history** <*index*>[**owner** <*string*>][**buckets** <*bucket-number*>][**interval** <*seconds*>]	This enables the history collection function of the interface.

4. To configure an event, use the following command.

Command	Function
ZXR10(config)#**rmon event** <*index*>[**log**][**trap** <*community*>][**description** <*string*>][**owner** <*string*>]	This configures an event.

5. To display RMON configuration and relevant information, use the following command.

Command	Function
ZXR10(config)#**show rmon** [**alarms**][**events**][**history**][**statistics**]	This displays RMON configuration and relevant information.

RMON Configuration Example

1. This example shows how to configure and start statistics control entries of the RMON.

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#rmon collection statistics 1 owner rmontest
ZXR10(config-gei_1/1)#
```

   Assume that n computers are linked to the port gei_1/1 and when these computers communicate on the sub-network. We can view traffic statistics data through NMS software and view RMON statistics information with the **show** command.

```
ZXR10#show rmon statistics
EtherStatsEntry 1 is active, and owned by rmontest
Monitors ifEntry.1.1 which has
Received 60739740 octets, 201157 packets,
1721 broadcast and 9185 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 32 collisions.
# of dropped packet events (due to lack of resources): 511
# of packets received of length (in octets):
64: 92955, 65-127: 14204, 128-255: 1116,
256-511: 4479, 512-1023: 85856, 1024-1518:2547
ZXR10#
```

2. This example shows how to configure and start history control entries of the RMON.

```
ZXR10(config)#interface gei_1/1
ZXR10(config-gei_1/1)#rmon collection history 1 bucket 10 interval
 10 owner rmontest
ZXR10(config-gei_1/1)#
```

   View RMON history information with the **show** command.

```
ZXR10#show rmon history
Entry 1 is active, and owned by rmontest
Monitors ifEntry.1.1 every 10 seconds
Requested # of time intervals, ie buckets, is 10
Granted # of time intervals, ie buckets, is 10
Sample # 1 began measuring at 00:11:00
Received 38346 octets, 216 packets,
0 broadcast and 80 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Network utilization is estimated at 1
```

3. This example shows how to configure and start alarm control entries of the RMON.

```
ZXR10(config)#rmon alarm 1 system.3.0 10 absolute
 rising-threshold 1000 1
                        Falling-threshold 10 1 owner rmontest
ZXR10(config)#
```

   View RMON alarm information with the **show** command.

```
ZXR10#show rmon alarm
Alarm 1 is active, owned by rmontest
Monitors system.3.0 every 10 seconds
Taking absolute samples, last value was 54000
Rising threshold is 1000, assigned to event 1
```

```
Falling threshold is 10, assigned to event 0
On startup enable rising or falling alarm
ZXR10#
```

4. This example shows how to configure and enable the event function.

```
ZXR10(config)#rmon event 1 log trap rmontrap
description test owner rmontest
ZXR10(config)#
```

Configure an alarm control entry and wait for 10s, and then view RMON event contents with the **show** command.

```
ZXR10#show rmon event
Event 1 is active, owned by rmontest
Description is test
Event firing causes log and trap to community rmontrap,
last fired 05:40:20
Current log entries:
        index       time   description
         1        05:40:14   test
ZXR10#
```

SysLog Configuration

SysLog Overview

ZXR10 5900/5200 provides users with log information setting and query functions. Log information provides convenient routine maintenance of the routing switch. User can view alarm information and port state change condition on the routing switch through log information. Log information can be displayed on the configuration terminal in real time or can be saved to a file on the routing switch or background log server. The syslog protocol can be enabled on ZXR10 5900/5200 so that the routers can communicate with the background syslog server to deliver the log information.

Configuring SysLog

1. To enable the log function, use the following command.

Command	**Function**
`ZXR10(config)#`**logging on**	This enables the log function.

2. To set the log buffer size, use the following command.

Command	**Function**
`ZXR10(config)#`**logging buffer** <*buffer-size*>	This sets the log buffer size.

3. To set log clearance mode, use the following command.

Command	Function
ZXR10(config)#**logging mode** <*mode*>[<*interval*>]	This sets log clearance mode.

4. To set the log level displayed on the console interface of telnet interface, use the following command.

Command	Function
ZXR10(config)#**logging console** <*level*>[**filter map-name**]	This sets the log level displayed on the console interface of telnet interface.

5. To set the log level saved in log buffer, use the following command.

Command	Function
ZXR10(config)#**logging level** <*level*>	This sets the log level saved in log buffer.

6. To set the background FTP log server parameter, use the following command.

Command	Function
ZXR10(config)#**logging ftp** <*level*>[**mng**]<*ftp-server*><*username*><*password*>[<*filename*>]	This sets the background FTP log server parameter.

7. To set parameters of alarm information which is sent to trap server, use the following command.

Command	Function
ZXR10(config)#**logging trap** <*level*><*community*>[**mng**]<*host-address*>	This sets parameters of alarm information which is sent to trap server.

8. To set parameters to pack information in alarm buffer to file and send it to ftp server, use the following command.

Command	Function
ZXR10(config)#**logging filesavetime** {**everyday** <*hh:mm:ss*>|**interval** <*hh:mm:ss*>|**month** <*monthday*><*hh:mmm:ss*>|**week** <*weekday*><*hh:mm:ss*>}[**mng**]<*ftp sever*><*username*><*password*><*alarm file prefix*>	This sets parameters to pack information in alarm buffer to file and send it to ftp server.

9. To set background syslog server parameters, use the following command.

Command	Function
ZXR10(config)#**syslog-server host** <*ip-address*>[**fport** <*fport*>][**lport** <*lport*>][**alarmlog**| **alarmlog**| **alarmlog**]	This sets background syslog server parameters.

10. To display log information, use the following command.

Command	Function
ZXR10(config)#**show logging alarm** {[**typeid** <*type*>][**start-date** <*date*>][**end-date** <*date*>][**level** <*level*>]}	This displays log information.

Now, the supported alarm information types contain ENVIRONMENT, BOARD, PORT, ROS, DATABASE, OAM, SECURITY, OSPF, RIP, BGP, DRP, TCP-UDP, IP, IGMP, TELNET, ARP, ISIS, ICMP, SNMP and RMON.

11. To save alarm logging information in location flash: data/log.dat, use the following command.

Command	Function
ZXR10#**write logging**	This saves alarm logging information in location flash: data/log.dat.

12. To configure packets, use the following command.

Command	Function
ZXR10#**syslog-server facility**	This distinguishes different servers by this field.

13. To designate source address in syslog, use the following command.

Command	Function
ZXR10#**syslog-server source** <*ip-address*>	This designates source address in syslog.

Syslog Configuration Example

The following is a system log setting example. When configuring, log function must be enabled with the **logging on** command .

```
ZXR10(config)#logging on
ZXR10(config)#logging buffer 100
ZXR10(config)#logging mode FULLCLEAR
ZXR10(config)#logging console warnings
ZXR10(config)#logging level errors
ZXR10(config)#logging ftp notificational 168.1.70.100
target target zxralarm.log
ZXR10(config)# syslog-server host 192.168.0.100
```

TACACS+ Configuration

TACACS+ Overview

TACACS+, Terminal Access Controller Access Control System, is the most popular AAA protocol which is the simplified name of Authorization, Authentication and Accounting. TACACS+ supports independent authentication, authorization and accounting, allowing different TACACS+ security server to be authentication, authorization and accounting server respectively.

PPP user and Telnet user that use the system service should be authenticated, authorized and accounted in ZXROS. TACACS+ protocol can solve this problem effectively. TACACS+ module provides centralized security authentication, authorization and accounting for logging user.

TACACS+ software module in ZXROS is client software authenticated by TACACS+. It implements the protocol interaction between NAS and TACACS+ security server to complete TACACS+ AAA function. TACACS+ client also provides the operation that TACACS+ configuration needs to configure TACACS+ environment.

At present, ZXR10 5900/5200 supports TACACS+ authentication to provide authentication of Telnet users accessing the routers.

ZXR10 5900/5200 supports multiple TACACS+ server groups. Each TACACS+ group permits the configuration of four authentication servers and each group can be configured with two parameters: server timeout time and retry times. The administrator can configure different TACACS+ server groups to select a specific TACACS+ server.

Configuring TACACS+

1. To enable TACACS+ protocol function, use the following command.

Command	Function
`ZXR10(config)#`**tacacs enable**	This enables TACACS+ protocol function.

2. To disable TACACS+ protocol function, use the following command.

Command	Function
`ZXR10(config)#`**tacacs disable** [**clear**]	This disables TACACS+ protocol function.

3. To configure TACACS+ server group member, use the following command.

Command	Function
ZXR10(config-sg)#**server** <*ip-addr*>[**port** <*1025~65535*>]	This configures TACACS+ server group member.

Command parameter description is as follows:

Parameter	Description
<*ip-addr***>**	IP address of TACACS + Server which must be the configured one.
<*1025~65535***>**	The port number that TCP connects.

4. To configure TACACS client IP address, use the following command.

Command	Function
ZXR10(config)#**tacacs-client** <*ip-addr*>[**port** <*1025~65535*>	This configures Tacacs+ client IP address which is used to communicate with Tacacs+ server. Configuration is deleted with no command.

Command parameter description is as follows:

Parameter	Description
<*ip-addr***>**	Client IP
<*1025~65535***>**	Client layer 4 port

5. To configure TACACS server parameter, use the following command.

Command	Function
ZXR10(config)#**tacacs-server host** <*ip-addr*>[**port** <*integer*>][**timeout** <*integer*>][**key** <*string*>]	This configures TACACS server parameter. Configuration is deleted with no command.

Command parameter description is as follows:

Parameter	Description
<*ip-addr***>**	TACACS + Server IP address
port	Port number for TCP connection. The default value is 49.
timeout	Connection timeout time, in range of 1~1000. Unit is second. The configuration here will invalidate the global configuration.
key	Encryption key between NAS and TACACS+ server. The configuration here will invalidate the global configuration.

6. To configure global TACACS+ protocol encryption key, use the following command.

Command	Function
ZXR10(config)#**tacacs-server key** <*key*>	This configures global TACACS+ protocol encryption key which is valid for all servers without designated key. Configuration is deleted with no command.

Command parameter description is as follows:

Parameter	Description
<*key*>	Encryption key used in exchanging packets between NAS and server. Length: 1~63 characters (without space). The key defined in the server must be same as this one.

7. To configure TACACS+ maximum packet length, use the following command.

Command	Function
ZXR10(config)#**tacacs-server packet** <*1024~4096*>	This configures TACACS+ maximum packet length. The default configuration 1024 is restored with no command.

Command parameter description is as follows:

Parameter	Description
<*1024~4096*>	Packet maximum length. The default is 1024.

8. To configure connection timeout for TACACS+ server, use the following command.

Command	Function
ZXR10(config)#**tacacs-server timeout** <*1~1000*>	This configures connection timeout for TACACS+ server. The default is 5s. The default configuration is restored with no command.

Command parameter description is as follows:

Parameter	Description
<*1~1000*>	timeout time, The unit is second. 1~1000, 5s by default.

9. To configure TACACS+ server group, use the following command.

Command	Function
ZXR10(config)#**aaa group server tacacs+** <*group-name*>	This enters into AAA server group configuration mode. Server group configuration is deleted with no command.

Command parameter description is as follows:

Parameter	Description
<*group-name***>**	tacacs+ server group name with 1~31 characters

TACACS Configuration Example

```
ZXR10(config)#tacacs enable
ZXR10(config)#tacacs-server host 1.1.1.1
ZXR10(config)#tacacs-client 1.1.1.2
ZXR10(config)#aaa authentication login default group zte
ZXR10(config)#aaa authentication enable default local group zte
ZXR10(config)#aaa authorization login default group zte
ZXR10(config)#user-authentication-type tacacs+
ZXR10(config)#user-authorization-type tacacs+
ZXR10(config)#aaa group-server tacacs+ zte
ZXR10(config-sg)#server 1.1.1.1
```

This page is intentionally blank.

Chapter 12

DOT1X Configuration

Table of Contents

DOT1x Overview

DOT1X, IEEE 802.1x, is a port-based network access control protocol. It optimizes the authentication mode and authentication architecture and solves the problems caused by traditional PPPoE and Web/Portal authentication modes, therefore it is more suitable for the broadband Ethernet.

IEEE 802.1x protocol architecture contains three major parts: Supplicant System, Authenticator System and Authentication Server System.

1. Generally client system is a user terminal system where client software is often installed. User originates IEEE802.1x protocol authentication by booting the client software. To support port-based access control, the client system needs to support the Extensible Authentication Protocol Over LAN (EAPOL).
2. Authentication system is network equipment supporting the IEEE802.1x protocol, such as the switch. The equipment corresponds to different user ports (physical port or MAC address, VLAN and IP of the user equipment) and has two logical ports composed of the controlled port and uncontrolled port.

   - Uncontrolled port is always in bidirectional connection state and delivers EAPOL protocol, which ensures the client to always send or receive authentication.
   - Controlled port opens upon success of the authentication to deliver network resources and services. The controlled port modes can be configured as bidirectional controlled and only transmission controlled to adapt to different application environments. If the user fails to pass authentication, the controlled port is in unauthenticated state and the user cannot access services offered by the authentication system.

   Controlled port and uncontrolled port in the IEEE 802.1x protocol are logical concepts and such physical switches are inexistent in the equipment. The IEEE 802.1x protocol establishes

a logical authentication channel for each user and other users cannot use the logical channel after the port is enabled.

3. Authentication server is usually a RADIUS server. In authentication server user-related information is stored such as the VLAN where the user locates, CAR parameter, priority and access control list of the user. Once the user passes authentication, the authentication server delivers user-related information to the authentication system which creates a dynamic access control list. The above parameters are used to measure subsequent traffic of the user. Authentication server and RADIUS server communicate with each other through the RADIUS protocol.

Configuring DOT1X

Configuring AAA

1. To create an AAA control entry, use the following command.

Command	Function
ZXR10(config-nas)#**create aaa** <*rule-id*>[**port** <*port-name*>][**vlan** <*vlan-id*>]	This creates an AAA control entry.

2. To clear an AAA control entry, use the following command.

Command	Function
ZXR10(config-nas)#**clear aaa** <*rule-id*>	This clears an AAA control entry.

3. To enable/disable dot1x authentication or trunk, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **control** {**dot1x**|**dot1x -relay**}{**enable**|**disable**}	This enables/disables dot1x authentication or trunk.

4. To select an authentication mode, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **authentication** {**local**|**radius**}	This selects an authentication mode.

5. To select an authentication protocol, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **protocol** {**pap**|**chap**|**eap**}	This selects an authentication protocol.

6. To configure the keepalive interval, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **keepalive** {**enable** [**period** < *period-value* >]|**disable**}	This configures the keepalive interval.

7. To configure whether to charge, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **accounting** {**enable**|**disable**}	This configures whether to enable accounting.

8. To configure whether multiple users are allowed and limitation on the number of users, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **multiple-hosts** {**enable** [**max-hosts** <*host-number*>]|**disable**}	This configures whether multiple users are allowed and limitation on the number of users.

9. To configure the default ISP server name, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **default-isp** <*isp-name*>	This configures the default ISP server name.

10. To configure whether to conduct full name accounting, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **fullaccount** {**enable**|**disable**}	This configures whether to conduct full name accounting.

11. To configure a group name, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **groupname** <*group-name*>	This configures a group name.

12. To bind an AAA control entry with the radius server group, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **radius-server authentication**< *group-number* >	This binds an AAA control entry with the radius server group.

13. To configure binding radius accounting server group, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **radius-server accounting** < *group-number* >	This configures binding radius accounting server group.

14. To configure authentication mode as local or radius server mode, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **authentication** {**local**|**radius**}	This configures authentication mode as local or radius server mode.

15. To configure authorization mode, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **authorization** {**auto**|**unauthorized**|**authorized**}	This configures authorization mode.

Configuring DOT1X Parameter

1. To configure dot1x period for re-authentication, use the following command.

Command	Function
ZXR10(config-nas)#**dot1x re-authentication** {**enable** [**period** < *period* >]|**disable**}	This configures dot1x period for re-authentication.

2. To configure the quiet period of dot1x authentication, use the following command.

Command	Function
ZXR10(config-nas)#**dot1x quiet-period** < *period* >	This configures the quiet period of dot1x authentication.

3. To configure the sending period of dot1x authentication, use the following command.

Command	Function
ZXR10(config-nas)#**dot1x tx-period** <*period*>	This configures the sending period of dot1x authentication.

4. To configure dot1x client timeout time, use the following command.

Command	Function
ZXR10(config-nas)#**dot1x supplicant-timeout** <*period*>	This configures dot1x client timeout time.

5. To configure dot1x authentication server timeout time, use the following command.

Command	Function
ZXR10(config-nas)#**dot1x server-timeout** <*period*>	This configures dot1x authentication server timeout time.

6. To configure the maximum times of requests for dot1x client, use the following command.

Command	Function
ZXR10(config-nas)#**dot1x max-requests** <*count*>	This configures the maximum times of requests for dot1x client.

Configuring Local Authentication User

1. To create a local user, use the following command.

Command	Function
ZXR10(config-nas)#**create localuser** <*user-id*>[**name** <*user-name*>][**password** <*user-password*>]	This creates a local user.

2. To delete a local user, use the following command.

Command	Function
ZXR10(config-nas)#**clear localuser** < *user-id* >	This deletes a local user.

3. To bind the user with the port, use the following command.

Command	Function
ZXR10(config-nas)#**localuser** <*user-id*> **port** <*port-name*>	This binds the user with the port.

4. To bind the user with the VLAN, use the following command.

Command	Function
ZXR10(config-nas)#**localuser** <*user-id*> **vlan** <*vlan-id*>	This binds the user with the VLAN.

5. To bind the user with the MAC address, use the following command.

Command	Function
ZXR10(config-nas)#**localuser** <*user-id*> **mac** <*mac-address*>	This binds the user with the MAC address.

6. To configure whether to charge the local user, use the following command.

Command	Function
ZXR10(config-nas)#**localuser** <*user-id*> **accounting** {**enable**|**disable**}	This configures whether to charge the local user.

Managing DOT1X Authentication Access User

1. To display all dot1x authentication users, use the following command.

Command	Function
ZXR10(config-nas)#**show clients** [**device** <*device-number*>| **index** <*client-index*>| **mac** <*mac-address*>| **port** <*port-name*>| **vlan** <*vlan-id*>]	This displays all dot1x authentication users.

2. To delete a specific user, use the following command.

Command	Function
ZXR10(config-nas)#**clear client** [**index** <*client-index*>|**port** <*port-name*>| **vlan** <*vlan-id*>]	This deletes a specific user.

Managing Multiple Domains Configuration

1. To enable/disable multiple domains function, use the following command.

Command	Function
ZXR10(config)#**domain-auth enable**	This enables multiple domains authentication function.
ZXR10(config)#**no domain-auth**	This disables multiple domains authentication function.

2. To configure domain separator, use the following command.

Command	Function
ZXR10(config)#**domaindelimiter** <*domaindelimiter*>	@, /, %, # or other characters.
ZXR10(config)#**no domaindelimiter**	This cancels domain separator configuration.

3. To configure domain information, use the following command.

Command	Function
ZXR10(config)#**domain** <*domain-id*>[**default**]	This configures domain information.
ZXR10(config)#**no domain** <*domain-id*>[**default**]	This cancels domain information.

4. To configure domain fullname authentication information, use the following command.

Command	Function
ZXR10(config-domain)#**domain-fullaccount enable**	This configures domain fullname authentication information.
ZXR10(config-domain)#**no domain-fullaccount**	This deletes domain fullname authentication information.

5. To configure domain name information, use the following command.

Command	Function
ZXR10(config-domain)#**domain-name** <*domain-name*>	This configures domain name information.
ZXR10(config-domain)#**no domain-name**	This deletes domain name information.

6. To configure domain accounting server information, use the following command.

Command	Function
ZXR10(config-domain)#**domain-radius-account-server** <*server-id*>	This configures domain accounting server information.
ZXR10(config-domain)#**no domain-radius-account-server**	This deletes domain accounting server information.

7. To configure domain authentication server information, use the following command.

Command	Function
ZXR10(config-domain)#**domain-radius-authen-server** <*server-id*>	This configures domain authentication server information.
ZXR10(config-domain)#**no domain-radius-authen-server**	This deletes domain authentication server information.

8. To configure ISP name in rule, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **default-isp** <*isp-name*>[**default**]	This configures ISP name in rule.
ZXR10(config-nas)#**no aaa** <*rule-id*> **default-isp** [<*isp-name*>]	This deletes ISP name in rule.

9. To configure domain name separator in rule, use the following command.

Command	Function
ZXR10(config-nas)#**aaa** <*rule-id*> **domaindelimiter** <*domaindelimiter*>	@, /, %, # or other characters.
ZXR10(config-nas)#**no aaa** <*rule-id*> **domaindelimiter**	This cancels domain separator in rule.

Configuring 802.1x VLAN Hopping

To configure VLAN hopping function at the interface, use the following command.

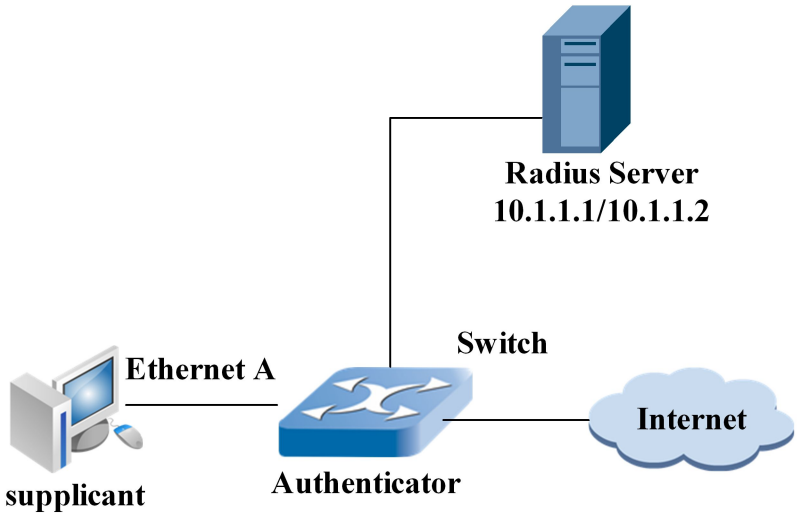
Command	Function
ZXR10(config-gei_1/x)#**vlanjump** {**enable**|**disable**}[**de faultauthvlan** <*vlan-id*>]	This configures VLAN hopping function at the specific interface.

DOT1X Configuration Example

Dot1x Radius Authentication Application

Workstation of a user is connected to Ethernet A of the Ethernet switch. This is shown in Figure 29.

FIGURE 29 DOT1X RADIUS AUTHENTICATION APPLICATION



The following needs to be implemented on the switch:

- Conduct user access authentication on each port to control the user's access to the Internet.
- It is required that the access control mode is MAC address-based access control mode.
- All the AAA access users belong to the default domain zte163.net.
- This authentication and RADIUS authentication are conducted at the same time.
- Disconnect the user and make it offline if RADIUS accounting fails.
- Do not add the domain name after the user name during access.
- Connect the server group composed of two RADIUS servers to the switch. IP addresses of these servers are 10.1.1.1 and 10.1.1.2 respectively. It is required that the former serves as the master authentication/slave charging server and the latter serves as the slave authentication/master charging server.

- Set the encryption password to "aaazte" when the system exchanges packets with the authentication RADIUS server. Set the system to resend packets to the RADIUS server if no response comes from this server within five seconds after the previous sending, and packets can be resent for five times at most. Direct the system to remove the user domain name from the user name and then send it to the RADIUS server.

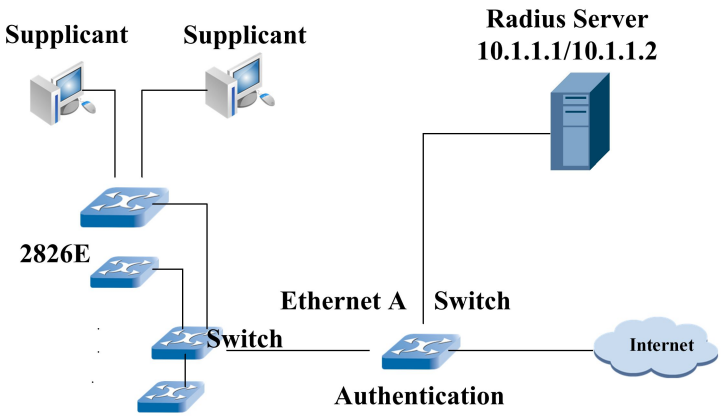
Switch configuration:

```
ZXR10(config)#radius authentication-group 1
ZXR10(config-authgrp-1)#server 1 10.1.1.1 key aaazte  port
<auth server port num >
ZXR10(config-authgrp-1)#server 2 10.1.1.2 key aaazte port
<auth server port num >
ZXR10(config-authgrp-1)#exit
ZXR10(config)#radius accounting-group 1
ZXR10(config-acctgrp-1)#server 1 10.1.1.1 key aaazte  port
<acct server port num >
ZXR10(config-acctgrp-1)#server 2 10.1.1.2 key aaazte port
<acct server port num >
ZXR10(config-acctgrp-1)#exit
ZXR10(config)# nas
ZXR10(config-nas)#dot1x re-authentication enable period 5
ZXR10(config-nas)#dot1x max-request 5
ZXR10(config-nas)#create aaa 1 port gei_1/1
ZXR10(config-nas)#aaa 1 authentication radius
ZXR10(config-nas)#aaa 1 control dot1x enable
ZXR10(config-nas)#aaa 1 authorization auto
ZXR10(config-nas)#aaa 1 accounting enable
ZXR10(config-nas)#aaa 1 multiple-hosts enable
ZXR10(config-nas)#aaa 1 default-isp zte163.net
ZXR10(config-nas)#aaa 1 fullaccount disable
ZXR10(config-nas)#aaa 1 radius-server authentication   1
ZXR10(config-nas)#aaa 1 radius-server accounting  1
ZXR10(config-nas)#aaa 1 authen radius
```

Dot1x Trunk Authentication Application

Internal network of an enterprise is shown in Figure 30.

FIGURE 30 DOT1X TRUNK AUTHENTICATION APPLICATION



The criteria is that Internet resources can only be accessed through the authentication host and only enterprise network resources can be accessed by other hosts.

- Divide the hosts in the enterprise into a sub-network (or multiple sub-networks), where the hosts can access each other.
- Enable the 802.1X trunk function on the Ethernet switch inside the sub-network and enable 802.1X authentication on the Ethernet port of the sub-network gateway.
- Do not charge users inside the enterprise, and only authenticate them on the Radius server. The master/slave authentication servers are 10.1.1.1/10.1.1.2 respectively. It is assumed that the enterprise uses the 2826E Ethernet switch inside it and gateway uses the ZXR10 5900/5200.

2826E configuration:

```
Set dot1xreley enable
```

ZXR10 5900/5200 configuration:

```
ZXR10(config)#radius authentication-group 1
ZXR10(config-authgrp-1)#server 1 10.1.1.1 key aaazte port 1812
ZXR10(config-authgrp-1)#server 2 10.1.1.2 key aaazte port 1812
ZXR10(config-authgrp-1)#exit
ZXR10(config)#nas
ZXR10(config-nas)#create aaa 1 port gei_1/1
ZXR10(config-nas)#aaa 1 control dot1x enable
ZXR10(config-nas)#aaa 1 authentication radius
ZXR10(config-nas)#aaa 1 authorization auto
ZXR10(config-nas)#aaa 1 accounting disable
ZXR10(config-nas)#aaa 1 multiple-hosts enable
ZXR10(config-nas)#aaa 1 default-isp zte163.net
ZXR10(config-nas)#aaa 1 fullaccount disable
ZXR10(config-nas)#aaa 1 radius-server authentication 1
```

Dot1x Local Authentication Application

In the applications shown in Figure 29 and Figure 30, the enterprise wants to register the network card address of each host. Only the MAC address of the network card is checked when the user uses any account to log in from the dot1x client. User can log in only when address is legal. In addition, enterprise numbers each MAC address and sums up Internet access duration of the user based on the number. ZXR10 5900/5200 can implement the application requirement. Authenticator adopts ZXR10 5900/5200, as shown in Figure 29and Figure 30, to implement the application configuration as follows:

```
ZXR10(config)#radius accounting-group 1
ZXR10(config-acctgrp-1)#server 1 10.1.1.1 key aaazte  port
 <auth server port num >
ZXR10(config-acctgrp-1)#server 2 10.1.1.2 key aaazte port
  <auth server port num >
ZXR10(config-acctgrp-1)#exit
ZXR10(config)#nas
ZXR10(config-nas)#create aaa 1 port gei_1/1
ZXR10(config-nas)#aaa 1 control dot1x enable
ZXR10(config-nas)#aaa 1 authentication local
ZXR10(config-nas)#aaa 1 authorization auto
ZXR10(config-nas)#aaa 1 accounting disable
```

```
ZXR10(config-nas)#aaa 1 multiple-hosts enable
ZXR10(config-nas)#aaa 1 default-isp zte163.net
ZXR10(config-nas)#aaa 1 fullaccount disable
ZXR10(config-nas)# aaa 1 radius-server accounting 1
ZXR10(config-nas)#create localuser 1 name  A0001
ZXR10(config-nas)#localuser 1 mac 00d0.d0d0.1234
ZXR10(config-nas)#localuser 1 accounting enable
ZXR10(config-nas)#create localuser 2 name  A0002
ZXR10(config-nas)#localuser 2 mac 00d0.d0d0.1456
ZXR10(config-nas)#localuser 2 accounting enable
ZXR10(config-nas)#create localuser 3 name  A0003
ZXR10(config-nas)#localuser 3 mac 00d0.d0d0.1689
ZXR10(config-nas)#localuser 3 accounting enable
```

In the above configuration, the local authentication function on the ZXR10 5900/5200 is enabled to implement the application requirement of the enterprise. According to the above configuration, only 00d0.d0d0.1234, 00d0.d0d0.1456 and 00d0.d0d0.1689 network card addresses can be accessed and the Internet access duration of these three users, named as A0001, A0002 and A0003, is summed up. The duration is recorded on the Radius server.

DOT1X Multiple Domains Function

In Figure 29 andFigure 30 applicationsGuest Vlan function is based on interface. When user authentication at the port succeeds, interface will be switched in authentication VLAN. and other users which are not unauthorized can't visit Guest Vlan internal resource. When all authentication users at the port are offline, port can recover attribute of Guest Vlan. If one authentication user exists on the port the port can't recover attribute of Guest Vlan. This application can be implemented on 5900/5200 switch. In Figure 29 and Figure 30 , authenticator applies 5900/5200, the configuration example of 5900/5200 is as follows.

```
ZXR10(config)#nas
ZXR10(config-nas)#create aaa 1 port gei_1/1
ZXR10(config-nas)#aaa 1 control dot1x enable
ZXR10(config-nas)#aaa 1 authentication local
ZXR10(config-nas)#create localuser 1 name  A0001
ZXR10(config-gei_1/1)# vlanjump enable defaultauthvlan 20
```

In the above configuration, local authentication function on 5900/5200 is applied to meet manager application requirement.

DOT1X Maintenance and Diagnosis

When encountering DOT1X problem, we can locate the fault and remove them with relevant debugging commands. Among these commands, **show** command and **debug** command may be used.

1. To display Dot1x authentication configuration information, use the following command.

   show dot1x

2. To view an AAA control entry, use the following command.

   show aaa

3. To display online user information, use the following command.

   show clients

4. To display configured local user information, use the following command.

   show localuser

Command **debug** can be used to trace packet sending, receiving and its processing during Dot1x Server/Relay process.

1. To trace the transceiving packet and handling processes of the dot1x, use the following command.

   debug nas

2. To trace the process of interacting with the radius, use the following command.

   debug radius

This page is intentionally blank.

Chapter 13

Cluster Management Configuration

Table of Contents

Cluster Management Overview

Cluster is a combination of a group of switches in a specific broadcast domain. This group of switches forms a unified management domain which provides a public network IP address and a management interface to the outside and provides the functions of managing and accessing every member in the cluster.

The management switch which configures public network IP address is called command switch and other managed switches are called member switches. Generally, public network IP address is not configured for the member switch but a private address is assigned to the member switch with similar DHCP function of the command switch. Command switch and member switch form a cluster (private network).

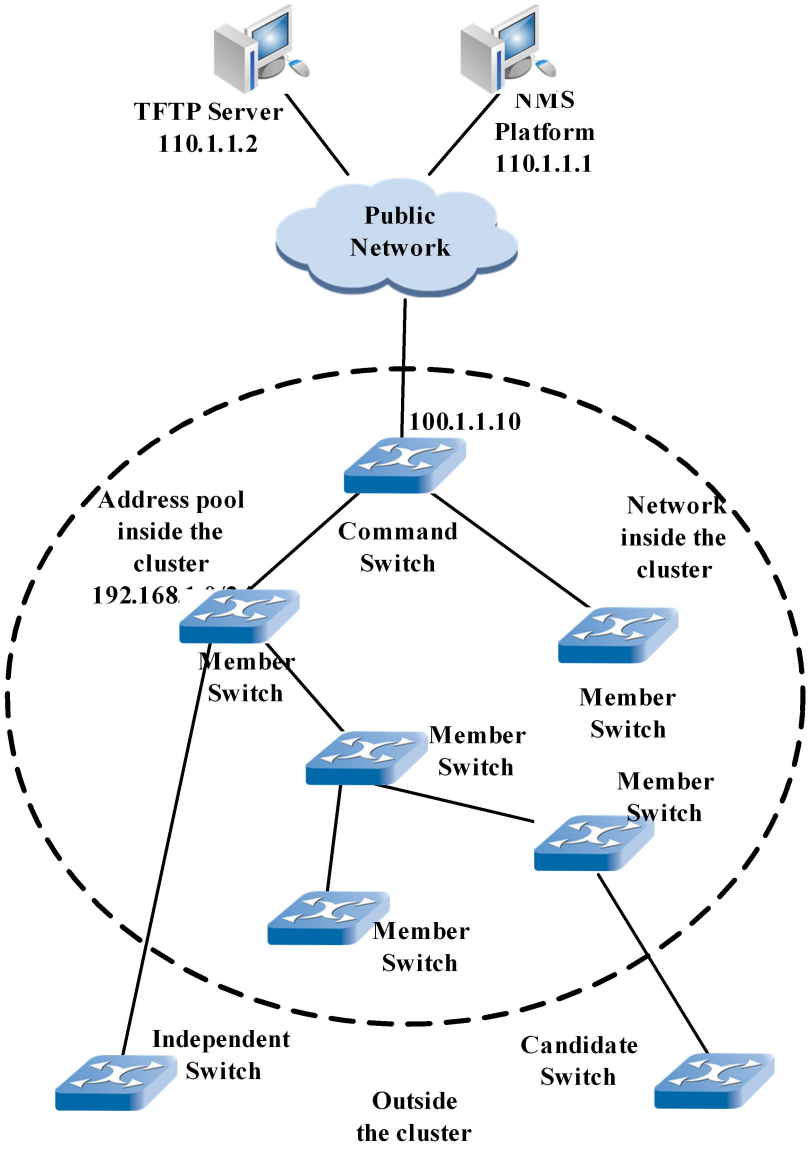
It is suggested to isolate the broadcast domain of the public network and that of the private network on the command switch, and shield the direct access to the private address. The command switch provides a management and maintenance channel to the outside to manage the cluster in a centralized and unified manner.

A broadcast domain is usually composed of four kinds of switches: command switch, member switch, candidate switch and independent switch.

There is only one command switch in a cluster. Command switch can collect equipment topology and establish a cluster automatically. After the cluster is established, command switch provides a management channel for cluster to manage member switch. Member switch serves as a candidate switch before being added into cluster. Switch which does not support cluster management is called independent switch.

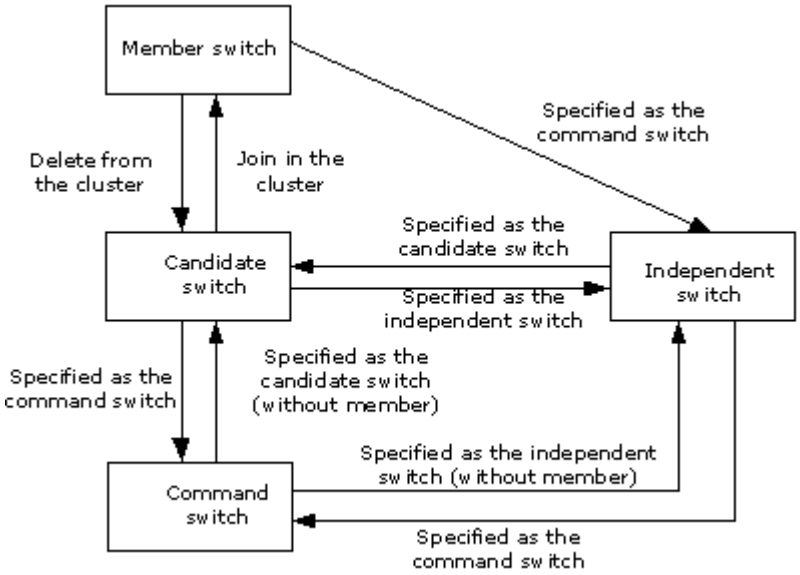
Cluster management network is formed as shown in Figure 31.

FIGURE 31 CLUSTER MANAGEMENT NETWORKING



Switching rule of four types switches in the cluster is shown in Figure 32.

FIGURE 32 SWITCH SWITCHING RULE



Configuring Cluster Management

Configuring ZDP Neighbor Discovery Protocol

1. To enable the ZDP function globally or in specific interface, use the following command.

Command	Function
ZXR10(config)#**zdp enable**	This enables the ZDP function globally or in specific interface.

2. To configure time interval of transmitting ZDP packets, use the following command.

Command	Function
ZXR10(config)#**zdp timer** <*time*>	This configures time interval of transmitting ZDP packets.

3. To configure the valid holding time of ZDP information, use the following command.

Command	Function
ZXR10(config)#**zdp holdtime** <*time*>	This configures the valid holding time of ZDP information.

Configuring ZTP Topology Collection Protocol

1. To enable the ZTP function globally or in specific interface, use the following command.

Command	Function
ZXR10(config)#**ztp enable**	This enables the ZTP function globally or in specific interface.

2. To conduct ZTP topology collection on different VLANs, use the following command.

Command	Function
ZXR10(config)#**ztp vlan** <*vlanId*>	This conducts ZTP topology collection on different VLANs.

3. To set the hops of ZTP topology collection, use the following command.

Command	Function
ZXR10(config)#**ztp hop** <*number*>	This sets the hops of ZTP topology collection.

4. To set each hop delay in sending ZTP protocol packets, use the following command.

Command	Function
ZXR10(config)#**ztp hop-delay** <*time*>	This sets each hop delay in sending ZTP protocol packets.

5. To set delay in sending ZTP protocol packets on the port, use the following command.

Command	Function
ZXR10(config)#**ztp port-delay** <*time*>	This sets delay in sending ZTP protocol packets on the port.

6. To conduct once topology collection, use the following command.

Command	Function
ZXR10(config)#**ztp start**	This conducts once topology collection.

7. To set ZTP timing topology collection time, use the following command.

Command	Function
ZXR10(config)#**ztp timer**	This sets ZTP timing topology collection time.

Establishing Cluster

1. To set the switch to command, candidate or independent switch, use the following command.

Command	Function
ZXR10(config)#**group switch-type** { **candidate** | **independent** | **(commander** [**(ip-pool** <*ip_addr*>**(** { **mask** <*ip_addr*>| **length** <*mask_len*>}] **)** }	This sets the switch to command, candidate or independent switch and allocates an IP address pool to cluster.

2. To change the cluster name, use the following command.

Command	Function
ZXR10(config)#**group name** <*name* >	This changes the cluster name.

3. To set the cluster handshake time, use the following command.

Command	Function
ZXR10(config)#**group handtime** <*time*>	This sets the cluster handshake time.

4. To set the holding time between the member and command switch on the command switch, use the following command.

Command	Function
ZXR10(config)#**group holdtime** <*time*>	This sets the holding time between the member and command switch on the command switch.

5. To add a specific equipment or MAC address as a member on the command switch, use the following command.

Command	Function
ZXR10(config)#**group member** { **((mac** <*mac_addr*> **)** [**member** <*mem_id*>] **)** | **(device** <*device_id*> **)** }	This adds a specific equipment or MAC address as a member on the command switch.

Maintaining Cluster

1. To restart the member on the command switch, use the following command.

Command	Function
ZXR10(config)#**group reset-member** { **all** |<*member_id*>}	This restarts the member on the command switch.

2. To save the member on the command switch, use the following command.

Command	Function
ZXR10(config)#**group save-member** { **all** |<*member_id*>}	This saves the configuration for member on the command switch.

3. To delete the member configuration file from the command switch, use the following command.

Command	Function
ZXR10(config)#**group erase-member** { **all** |<*member_id*>}	This deletes the member configuration file from the command switch.

4. To configure the tftp server on the cluster, use the following command.

Command	Function
ZXR10(config)#**group tftp-server** <*ip_addr*>	This configures the tftp server on the cluster.

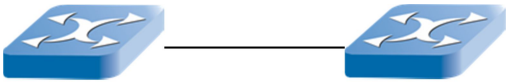
5. To configure the alarm receiver on the cluster, use the following command.

Command	Function
ZXR10(config)#**group trap-host** <*ip_addr*>	This configures the alarm receiver on the cluster.

Cluster Management Configuration Example

Connect two devices to implement cluster management, as shown in Figure 33.

FIGURE 33 CLUSTER MANAGEMENT CONFIGURATION



Configuration steps are as follows:

1. Ensure that two ports are in a VLAN (configured as vlan1 and ensure that vlan1 does not configure Layer 3 address).
2. Execute show zdp neighbor on DUT A and ensure zdp neighbor is already set up.
3. Execute ztp start on DUT A to conduct topology collection, and then execute show ztp device-list to view DUT A and DUT B.
4. Configure DUT A as the command switch with group switch-type command. View whether DUT A has become the command switch with show group command.
5. Configure DUT B as the member switch with group member device 1 command and then view Member 1 in the up state with the show group member command on DUT A.
6. Log in to Member 1 with the rlogin member 1 command in the privilege mode, and log in from Member 1 to the command switch with the rlogin commander command on DUT A.

Cluster Management Maintenance and Diagnosis

When encountering cluster management problem, we can locate the fault and remove them with relevant debugging commands. Among these commands, **show** command and **debug** command may be used.

Command **show** can be used to view current cluster configuration information.

1. To display ZDP configuration information, use the following command.

   show zdp

2. To view ZTP configuration information, use the following command.

   show ztp

3. To display cluster configuration information, use the following command.

show group

4. To display ZDP neighbor, use the following command.

   show zdp neighbour [**interface** <*interface*>| **mac** <*mac-address*>]

5. To display received equipment information, use the following command.

   show ztp {**device-list** | **device** {**mac** <*mac-address*>|<*id*>}}

6. To display group member information, use the following command.

   show group {**member** | **candidates** [**mac** <*mac-address*>]}

Command **debug group-management** can be used to trace packet sending, receiving of ZDP and ZTP and its processing during cluster management process.

Chapter 14

IPTV Configuration

Table of Contents

Internet Protocol Television Overview

Internet Protocol television (IPTV) is also called Interactive Network TV. IPTV is a method of distributing television content over IP that enables a more customized and interactive user experience. IPTV could allow people who were separated geographically to watch a movie together, while chatting and exchanging files simultaneously. IPTV uses a two-way broadcast signal sent through the provider's backbone network and servers, allowing viewers to select content on demand, and take advantage of other interactive TV options. IPTV can be used through PC or "IP machine box + TV".

Configuring IPTV

Configuring IPTV Global Parameters

1. To set the least preview time, use the following command.

Command	Function
`ZXR10(config-nas)#`**iptv control login-time**	This sets the least preview time.

2. To set the max preview counts on global, use the following command.

Command	Function
ZXR10(config-nas)#**iptv control prvcount count**	This sets the max preview counts on global.

3. To set the least preview interval on global, use the following command.

Command	Function
ZXR10(config-nas)#**iptv control prvinterval**	This sets the least preview interval on global.

4. To set the max preview time on global, use the following command.

Command	Function
ZXR10(config-nas)#**iptv control prvtime**	This sets the max preview time on global.

5. To set the period of global reset preview counts, use the following command.

Command	Function
ZXR10(config-nas)#**iptv control prvcount reset-period**	This sets the period of global reset preview counts.

6. To enable/disable IPTV, use the following command.

Command	Function
ZXR10(config-nas)#**iptv control {enable|disable}**	This enables/disables IPTV.

Configuring IPTV Channels

1. To create channels of IPTV, use the following command.

Command	Function
ZXR10(config)#**create iptv channel** [**general** <*256*>| **special** <*0-255*>]	This creates channels of IPTV.

Channel number is 0~256. 0~255 are special channels. Each channel must designate a multicast address. 256 is general channel and needn't to designate multicast address.

2. To set the name of a channel, use the following command.

Command	Function
ZXR10(config)#**iptv channel** <*0-256*> **name**	This sets the name of a channel.

3. To set a channel belonging to a multicast Vlan, use the following command.

Command	Function
ZXR10(config)#**iptv channel** <*0-256*> **mvlan**	This sets a channel belonging to a multicast Vlan.

4. To delete a channel, use the following command.

Command	Function
ZXR10(config)#**clear iptv channel**<*0-256*>	This deletes a channel.

Configuring Channel Access Control (CAC)

1. To create rules of CAC, use the following command.

Command	Function
ZXR10(config)#**create iptv cac-rule**<*1-256*>	This creates rules of CAC.

2. To set the name of CAC rule, use the following command.

Command	Function
ZXR10(config)#**iptv cac-rule** <*1-256*> **name**	This sets the name of CAC rule.

3. To set maximum preview counts of rules, use the following command.

Command	Function
ZXR10(config)#**iptv cac-rule** <*1-256*> **prvcount**	This sets maximum preview counts of rules. The default is global maximum preview count.

4. To set maximum preview time of rules, use the following command.

Command	Function
ZXR10(config)#**iptv cac-rule** <*1-256*> **prvtime**	This sets maximum preview time of rules. The default is global maximum preview time.

5. To set the least preview interval of rules, use the following command.

Command	Function
ZXR10(config)#**iptv cac-rule** <*1-256*> **prvinterval**	This sets the least preview interval of rules. The default is global least preview interval.

6. To set the right rule to channel, use the following command.

Command	Function
ZXR10(config)#**iptv cac-rule** <*1-256*> **right**	This sets the right rule to channel.

7. To delete rules, use the following command.

Command	Function
ZXR10(config)#**clear iptv cac-rule** <*1-256*>	This deletes rules.

Configuring Administrative Command of IPTV Users

Command	Function
ZXR10(config)#**clear iptv client**	This deletes online users of IPTV.

IPTV Configuration Example

1. User which connects to port gei_1/1 is a requesting user of multicast group 224.1.1.1. Vlan ID of this multicast group is 100. Configuration is shown below:

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right order 1
```

2. User which connects to port gei_1/1 in Vlan 1 is the preview user of multicast group 224.1.1.1. Max preview time is 2 minutes. Least preview interval is for 20 seconds. Max preview counts are 10. Vlan ID of multicast group is 100. Configuration is shown below:

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1 vlan 1
ZXR10(config-nas)# iptv cac-rule 1 prvcount 10
ZXR10(config-nas)# iptv cac-rule 1 prvtime 120
```

```
ZXR10(config-nas)# iptv cac-rule 1 prvinterval 20
ZXR10(config-nas)# iptv cac-rule 1 right preview 1
```

3. User which connects to port gei_1/1 wants to view all multicast groups in Vlan 100. Configuration is shown below:

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel general 256
ZXR10(config-nas)# iptv channel 256 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right order 256
```

4. Port gei_1/1 only permits receiving the requesting packets of multicast group 224.1.1.1. Vlan ID of this multicast group is 100. Configuration is shown below:

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right query 1
```

IPTV Maintenance and Diagnosis

1. To display the global configuration information of IPTV, use the following command.

   show iptv control

2. To display the channel information of IPTV, use the following command.

   show iptv channel [{ **id** <*channelno*>| **name**<*channel-name*>}]

3. To display the CAC rule, use the following command.

   show iptv cac-rule [{ **id** <*channelno*>| **name**<*channel-name*>}]

4. To display online users of IPTV, use the following command.

   show iptv client [{**port**<*portno*>| **vlan** <*vlanid*>| **device** <*devno*>}]

This page is intentionally blank.

Chapter 15

VBAS Configuration

Table of Contents

VBAS Overview

VBAS is the abbreviation of Virtual Broadband Access Server. It is an extent inquiry protocol between IP-DSLAM and BRAS equipment. The communication method between IP-DSLAM and BRAS is layer 2 point-to-point, that is, interface information inquiry and response packets are encapsulated in layer 2 Ethernet data frame.

The principle is to configure DSLAMDigital Subscriber Line Access Multiplexer) corresponding to VLAN on BAS. During the procedure of PPPOE calling, DSLAM applies VBAS protocol, that is, mapping to corresponding DSLAM according to VLAN of user. BAS demand the user line identity inquiry from DSLAM. In this user manual, switch means DSLAM equipment.

VBAS protocol is implemented by sending VBAS packet between BAS and DSLAM.

Configuring VBAS

Enabling/Disabling VBAS

Command	Function
`ZXR10(config)#`**vbas enable**	This enables VBAS.
`ZXR10(config)#`**no vbas enable**	This disables VBAS.

Enabling/Disabling VBAS in VLAN Mode

Step	Command	Function
1	`ZXR10(config)#`**vlan** <*vlan-id*>	This enters into VLAN Configuration Mode.
2	`ZXR10(config-vlanX)#` **vbas enable**	This enables VBAS in VLAN configuration mode.

Configuring VBAS Trust Interface

Step	Command	Function
1	`ZXR10(config)#`**interface** <*interface-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**vbas trust**	This configures VBAS trust interface.

Configuring VBAS Interface as User Interface or Network Interface

Step	Command	Function
1	`ZXR10(config)#`**interface** <*interface-name*>	This enters interface configuration mode.
2	`ZXR10(config-gei_1/x)#`**vbas port-type** {**user**|**net**}	This configures VBAS interface as user interface or network interface.

VBAS Configuration Example

Enable VBAS on the switch and configure VBAS enable vlan as vlan 1. Configure gei_1/1 as trust interface and interface type is user. Configuration is shown below:

```
ZXR10(config)#vbas enable
ZXR10(config)#vlan 1
ZXR10(config-vlan1)#vbas enable
ZXR10(config-vlan1)#exit
ZXR10(config)#interface gei_1/1
```

```
ZXR10(config-gei_1/1)#vbas trust
ZXR10(config-gei_1/1)#vbas port-type user
```

Note:

In this example, vlan1 which enables VBAS should include at least two interfaces, one connection user and another BRAS enquipment. In this example gei_1/1 is used to connect BRAS equipment.

VBAS Maintenance and Diagnosis

On the privileged mode, the command **debug vbas** is used to open VBAS debug function and send VBAS debug information.

This page is intentionally blank.

Chapter 16

ZESR/ZESR+ Configuration

Table of Contents

ZESR/ZESR+ Overview

ZESRZTE Ethernet Smart Ringis a solution for solving the layer 2 loop problem (RFC 3619). Compared with STP, the biggest advantage is that the link will switch and recover quickly when one way is disconnected and the shortest time is 50ms.

ZESR is applicable with multi-ring area. Multi-ring is designated that every level is an independent ring and low-level has two entry points to connect with high-level ring. The highest level ring is named as major-level ring and others are named as access rings. Multi-area is named that there are many protection instances on the same ring suitable to different service vlan. Their logic routes are different and independent.

ZESR+ , in double nodes double uplinks networking, improves the current ZESR to meet redundancy protection for uplink and node at the same time in double nodes double uplinks networking.

Configuring ZESR/ZESR+

Configuring ZESR Area Protection Instance

Step	Command	Function
1	ZXR10(config)#**zesr ctrl-vlan** *<1-4094>* **protect-instance** *<<0-16>*	<1-4094> area control vlan, indicates zesr area, < 0-16>the protected instance ID ,samed as stp instance
2	ZXR10(config)#**no zesr ctrl-vlan** *<1-4094>* **protect-instance**	<1-4094> area control vlan, indicates zesr area

ZESR protection instance is same as STP. Service vlan is put into protection instance, so generally enabling STP to cooperate with ZESR. Control vlan should use vlan except service and shouldn't conflict with service and network management. Note that pvid of the port shouldn't be selected as control vlan. Outside port shouldn't be put into control vlan.

Example

1. This example shows how to configure control vlan as 4000 protection instance as 1.
   ```
   ZXR10(config)# zesr ctrl-vlan 4000 protect-instance 1
   ```
2. This example shows how to delete control vlan as 4000 protection instance
   ```
   ZXR10(config)# no zesr ctrl-vlan 4000 protect-instance
   ```

Configuring Major-level Ring ZESR

To configure ZESR/ZESR+ on major-level ring , use the following commands. Major-level ring is the highest level ring, others are access rings.

Step	Command	Function
1	ZXR10(config)#**zesr ctrl-vlan** < *1-4094*> **major-level** {**(preforward** <*1-600*>[**preup** <*0-500*>]**)**| **(role** {**master** |**transit**|**zess-master**|**zess-transit**}	This configures major-level ring ZESR.
2	ZXR10(config)#**no zesr ctrl-vlan** < *1-4094*> **major-level**	This cancels the configuration of major-level ring ZESR.

Parameter Description:

Parameter	Description
< 1-4094>	Area control vlan, indicating zesr area

Parameter	Description
<1-600>	Preforward value, the unit is second. After the disconnected port reconnecting, unless ZESR protocol is set or after waiting for preforward time open automatically and the default is 10s.
<0-500>	Preup value, the unit is second. After Master detects that loop is up, the status is switched until delaying preup time. The default value is 0.
<primary-interface-name> <secondary-interface-name>	major ring two interfaces. To master, secondary interface is blocked to ensure ring is disconnected and no storm.
< 1-6>	Hello value, the unit is second. the time of master/zess-transit major interface sending hello protocol message, the default is 1s.
< 3-18>	The maximum time daley that master/zess-transit hasn't received hello packet. The unit is second. The default value is 3s.
master|transit|zess-master|zess-transit	configuration node role, master|transit is ZESR master node/transit node, zess-master|zess-transit is ZESR+ master node/transit node.

After node role and interface are ensured, preforward and preup can be configured, of which hello, fail and preup only can be used for master or zess-tranist, preup only can be configured as master or zess-master. Interface must be configured in control vlan before it is configured. Interface can use lacp interface but must be dynamic lacp and member interface must close stp.

Besides secondery interface of zess-master node decides blocking location. Therefore the interface must be placed on the uplink which need to be blocked, but secondery interface of zess-transit is suggested to be placed on uplink.

Example

1. This example shows how to configure control vlan as 4000, role as master, interface as gei_2/10 and gei_2/20.
```
ZXR10(config)# zesr ctrl-vlan 4000 major-level role master
 gei_2/10 gei_2/20
```
2. This example shows how to configure control vlan as 4000, role as zess-master, interface as gei_2/10 and gei_2/20.
```
ZXR10(config)# zesr ctrl-vlan 4000 major-level role zess-master
gei_2/10 gei_2/20
```
3. This example shows how to configure control vlan as 4000, role as master, preforward as 20s, preup as 20s.
```
ZXR10(config)#zesr ctrl-vlan 4000 major-level preforward 20 preup 20
```
4. This example shows how to configure control vlan as 4000, role as master, hello as 2s, fail as 4s.
```
ZXR10(config)#zesr ctrl-vlan 4000 major-level hello 2 fail 4
```

Configuring Access Ring ZESR

Step	Command	Function
1	ZXR10(config-router)#**zesr ctrl-vlan** < *1-4094*> **level** <*1-2*> **seg** <*1-4*>{**preforward** <*1-600*>[**preup** <*0-500*>]| **role** {**master** |**transit**}<*primary-interface-name*><*secondary-interface-name*>| { **edge-assistant**	**edge-control**}<*edge-interface-name*>}| **hello** < *1-6*> **fail** < *3-18*>}	This configures access ring ZESR.
2	ZXR10(config)#**no zesr ctrl-vlan** < *1-4094*> **level** <*1-2*> **seg** <*1-4*>	This cancels the configuration of access ring ZESR.

Parameter description

< 1-4094> Area control vlan, indicating zesr area

<1-2> Level of access ring

<1-4> access ring SN, at most 4 access rings in each level.

<1-600> Preforward value, the unit is second. After the disconnected port reconnecting, unless ZESR protocol is set or after waiting for preforward time open automatically and the default is 10s.

<0-500> Preup value, the unit is second. After Master or edge-control detects that loop is up, the status is switched until delaying preup time. The default value is 0.

<primary-interface-name> <secondary-interface-name> access ring two interfaces.

< 1-6> Hello value, the unit is second. The default is 1s.

< 3-18> The maximum time dalay that master or edge-control hasn't received hello packet. The unit is second. The default value is 3s.

<edge-interface-name> edge node interface

Switch could be in the entry that major-ring and access ring connect. At that time, it can be in major-ring or access ring . There are two interfaces in major-ring and one interface in access ring . Switch is named as entry node. The entry node could be edge-assistant and edge-control in access ring and edge-control plays a general node master role.

Example

1. This example shows how to configure control vlan as 4000, role as master, level as 1 , seg as 1, ports as gei_2/10 gei_2/10
```
ZXR10(config)# zesr ctrl-vlan 4000  level 1 seg 1 role
master gei_2/10 gei_2/20
```
2. This example shows how to configure control vlan as 4000, role as edge-assistant, level as 1 , seg as 1, ports as gei_2/1/10
```
ZXR10(config)# zesr ctrl-vlan 4000  level 1 seg 1 role
edge-assistant gei_2/1/10
```
3. This example shows how to configure control vlan as 4000, level as 1, seg as 1, preforward as 20s, preup as 20s
```
ZXR10(config)#zesr ctrl-vlan 4000 level 1 seg 1
preforward 20 preup 20
```
4. This example shows how to configure control vlan as 4000, level as 1, seg as 1, hello as 2s, fail as 4s
```
ZXR10(config)#zesr ctrl-vlan 4000 level 1 seg 1  hello 2 fail 4
```

Configuring ZESR Restart-Time

Command	Function
ZXR10(config)#**zesr restart-time** *<30-600>*	<30-600>the specific timethe unit is second, the default is 120s

Example This example shows how to configure ZESR restart-time as 60s.

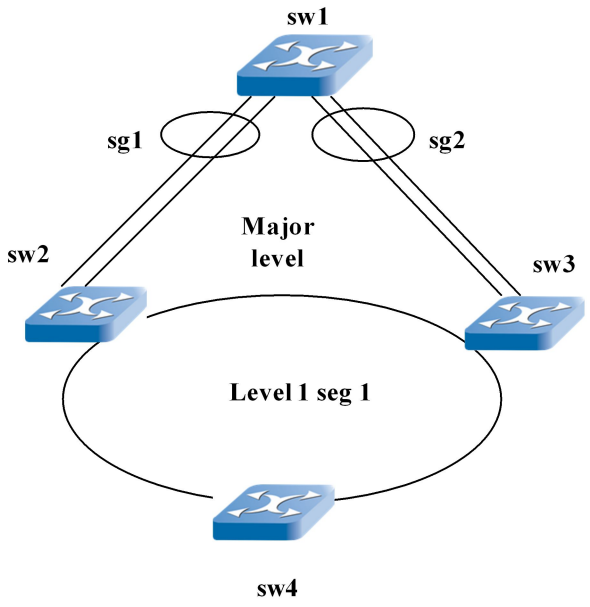
```
ZXR10(config)#zesr restart-time 60
```

ZESR/ZESR+ Configuration Example

ZESR Configuration Example

As shown in Figure 34,

FIGURE 34 ZESR CONFIGURATION EXAMPLE



SW1-SW4 buildup ring network, transparently transform 100-200, SW1 is core switch and the entire network exit. SW2-SW4 are convergence switch. Demand that service is not be affected if any link is down.

SW1: sg1gei_1/1, gei_1/2connects SW2, sg2gei_1/3, gei_1/4connects SW3

SW2: gei_1/1 connects SW3, gei_1/2 connects SW4, sg2gei_1/3, gei_1/4connects SW1

SW3: gei_1/1 connects SW2, gei_1/2 connects SW4, sg2gei_1/3, gei_1/4connects SW1

SW4: gei_1/1 connects SW2, gei_1/2 connects SW3.

The network formed by SW1, SW2 and SW3 is major level. SW2 is master node. The port that SW2 connect with SW1 is major port (sg1). The network formed by SW2-SW4 is slave ring level 1 seg 1. Take SW4 as master node and select the port connects with SW3 as slave port (gei_1/2), control vlan as 4000.

SW1 configuration:

```
ZXR10_S1(config)#spanning-tree enable
ZXR10_S1(config)#spanning-tree mst configuration
ZXR10(config-mstp)# instance 1 vlan 100-200
ZXR10(config-mstp)#exit

ZXR10_S1(config)#interface smartgroup1
ZXR10_S1(config-smartgroup1)#switchport mode trunk
ZXR10_S1 (config-smartgroup1)#smartgroup mode 802.3ad
ZXR10_S1(config-smartgroup1)switchport trunk vlan 100-200
ZXR10_S1(config-smartgroup1)switchport trunk vlan 4000
ZXR10_S1(config-smartgroup1)exit

ZXR10_S1(config)#interface smartgroup2
ZXR10_S1(config-smartgroup2)#switchport mode trunk
ZXR10_S1 (config-smartgroup2)#smartgroup mode 802.3ad
ZXR10_S1(config-smartgroup2)#switchport trunk vlan 100-200
ZXR10_S1(config-smartgroup2)#switchport trunk vlan 4000
ZXR10_S1(config-smartgroup2)#exit

ZXR10_S1(config)#interface gei_1/1
ZXR10_S1(config-gei_1/1)#negotiation auto
ZXR10_S1(config-gei_1/1)#switchport mode trunk
ZXR10_S1(config-gei_1/1)#switchport trunk vlan 100-200
ZXR10_S1(config-gei_1/1)#switchport trunk vlan 4000
ZXR10_S1(config-gei_1/1)#smartgroup 1 mode active
ZXR10_S1(config-gei_1/1)#spanning-tree disable
ZXR10_S1(config-gei_1/1)#exit

ZXR10_S1(config)#interface gei_1/2
ZXR10_S1(config-gei_1/2)#negotiation auto
ZXR10_S1(config-gei_1/2)#switchport mode trunk
ZXR10_S1(config-gei_1/2)#switchport trunk vlan 100-200
ZXR10_S1(config-gei_1/2)#switchport trunk vlan 4000
ZXR10_S1(config-gei_1/2)#smartgroup 1 mode active
ZXR10_S1(config-gei_1/2)#spanning-tree disable
ZXR10_S1(config-gei_1/2)#exit

ZXR10_S1(config)#interface gei_1/3
ZXR10_S1(config-gei_1/3)#negotiation auto
ZXR10_S1(config-gei_1/3)#switchport mode trunk
ZXR10_S1(config-gei_1/3)#switchport trunk vlan 100-200
ZXR10_S1(config-gei_1/3)#switchport trunk vlan 4000
ZXR10_S1(config-gei_1/3)#smartgroup 2 mode active
ZXR10_S1(config-gei_1/3)#spanning-tree disable
ZXR10_S1(config-gei_1/3)#exit

ZXR10_S1(config)#interface gei_1/4
ZXR10_S1(config-gei_1/4)#negotiation auto
ZXR10_S1(config-gei_1/4)#switchport mode trunk
ZXR10_S1(config-gei_1/4)#switchport trunk vlan 100-200
ZXR10_S1(config-gei_1/4)#switchport trunk vlan 4000
ZXR10_S1(config-gei_1/4)#smartgroup 2 mode active
ZXR10_S1(config-gei_1/4)#spanning-tree disable
ZXR10_S1(config-gei_1/4)#exit
```

```
ZXR10_S1(config)zesr ctrl-vlan 4000 protect-instance 1
ZXR10_S1(config)zesr ctrl-vlan 4000 major level role transit
smartgroup1 smartgroup2
```

SW2 Configuration

```
ZXR10_S2(config)#spanning-tree enable
ZXR10_S2(config)#spanning-tree mst configuration
ZXR10(config-mstp)# nstance 1 vlan 100-200
ZXR10(config-mstp)#exit

ZXR10_S2(config)#interface smartgroup1
ZXR10_S2(config-smartgroup1)switchport mode trunk
ZXR10_S2 (config-smartgroup1)#smartgroup mode 802.3ad
ZXR10_S2(config-smartgroup1)switchport trunk vlan 100-200
ZXR10_S2(config-smartgroup1)switchport trunk vlan 4000
ZXR10_S2(config-smartgroup1)exit

ZXR10_S2(config)#interface gei_1/1
ZXR10_S2(config-gei_1/1)switchport mode trunk
ZXR10_S2(config-gei_1/1)switchport trunk vlan 100-200
ZXR10_S2(config-gei_1/1)switchport trunk vlan 4000
ZXR10_S2(config-gei_1/1)exit

ZXR10_S2(config)#interface gei_1/2
ZXR10_S2(config-gei_1/2)switchport mode trunk
ZXR10_S2(config-gei_1/2)switchport trunk vlan 100-200
ZXR10_S2(config-gei_1/2)switchport trunk vlan 4000
ZXR10_S2(config-gei_1/2)exit

ZXR10_S2(config)#interface gei_1/3
ZXR10_S2(config-gei_1/3)negotiation auto
ZXR10_S2(config-gei_1/3)switchport mode trunk
ZXR10_S2(config-gei_1/3)switchport trunk vlan 100-200
ZXR10_S2(config-gei_1/3)switchport trunk vlan 4000
ZXR10_S2(config-gei_1/3)smartgroup 1 mode active
ZXR10_S2(config-gei_1/3)spanning-tree disable
ZXR10_S2(config-gei_1/3)exit

ZXR10_S2(config)#interface gei_1/4
ZXR10_S2(config-gei_1/4)negotiation auto
ZXR10_S2(config-gei_1/4)switchport mode trunk
ZXR10_S2(config-gei_1/4)switchport trunk vlan 100-200
ZXR10_S2(config-gei_1/4)switchport trunk vlan 4000
ZXR10_S2(config-gei_1/4)smartgroup 1 mode active
ZXR10_S2(config-gei_1/4)spanning-tree disable
ZXR10_S2(config-gei_1/4)exit

ZXR10_S2(config)#zesr ctrl-vlan 4000 protect-instance 1
ZXR10_S2(config)#zesr ctrl-vlan 4000 major level role transit
 smartgroup1 gei_1/1
ZXR10_S2(config)#zesr ctrl-vlan 4000 level 1 seg 1 role
edge- assistant gei_1/2
```

SW3 Configuration

Interface instance configuration is as SW2

```
ZXR10_S3(config)#zesr ctrl-vlan 4000 protect-instance 1
ZXR10_S3(config)#zesr ctrl-vlan 4000 major level role master
 smartgroup1 gei_1/1
ZXR10_S3(config)#zesr ctrl-vlan 4000 level 1 seg 1 role
edge- assistant gei_1/2
```

SW4 configuration

Interface instance configuration is as SW2

```
ZXR10_S4(config)#zesr ctrl-vlan 4000 protect-instance 1
ZXR10_S4(config)#zesr ctrl-vlan 4000 level 1 seg 1 role master
 gei_1/1 gei_1/2
```

ZESR and ZESR+ Hybrid Configuration Example

FIGURE 35 ZESR+ AND ZESR HYBRID NETWORKING TOPOLOGY FIGURE

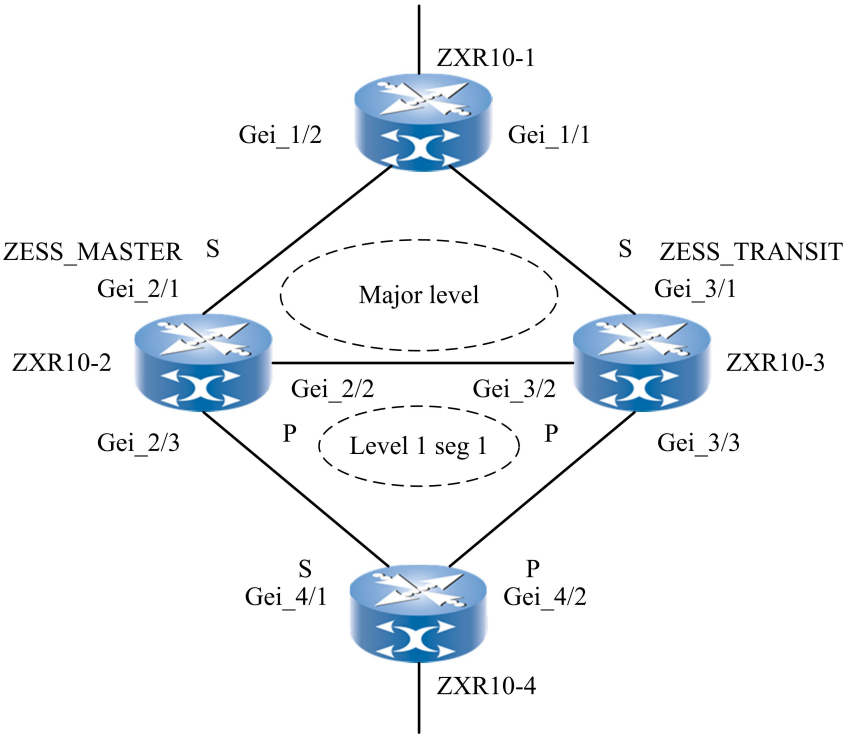


Figure 35 is typical ZESR+ and ZESR hybrid networking topology figure. Node ZXR10-2 , ZXR10-3 and ZXR10-1 form double nodes double uplinks, that is ZESR+. Also three nodes form a main loop virtually. Node ZXR10-2, ZXR10-3 and ZXR10-4 form a level 1seg 1 secondary ring, that is ZESR.

Node 1 configuration:

```
//as a normal switch, the major function is to
transparently transmit data package
//VLAN information need to be configured.
(port with tagged belongs to ctrl-vlan)
//close port broadcast and unknown unicast suppression
//connect ZXR10-3
ZXR10_S1(config)#interface gei_1/1
//configure interface working mode as auto negotiation
ZXR10_S1(config-gei_1/1)#negotiation auto
ZXR10_S1(config-gei_1/1)#switchport mode trunk
ZXR10_S1(config-gei_1/1)#switchport trunk vlan 100-200
ZXR10_S1(config-gei_1/1)#switchport trunk vlan 4000
ZXR10_S1(config-gei_1/1)#exit
 //connect ZXR10-2
ZXR10_S1(config)#interface gei_1/2
//configure interface working mode as auto negotiation
ZXR10_S1(config-gei_1/2)#negotiation auto
ZXR10_S1(config-gei_1/2)#switchport mode trunk
ZXR10_S1(config-gei_1/2)#switchport trunk vlan 100-200
ZXR10_S1(config-gei_1/2)#switchport trunk vlan 4000
ZXR10_S1(config-gei_1/2)#exit
```

Node 2 configuration:

```
//configure ZESR+ Master node
ZXR10_S2(config)#spanning-tree enable
ZXR10_S2(config)#spanning-tree mst configuration
ZXR10(config-mstp)# instance 1 vlan 100-200
ZXR10(config-mstp)#exit
 //connect ZXR10-1
ZXR10_S2(config)#interface gei_2/1
ZXR10_S2(config-gei_2/1)switchport mode trunk
ZXR10_S2(config-gei_2/1)switchport trunk vlan 100-200
ZXR10_S2(config-gei_2/1)switchport trunk vlan 4000
ZXR10_S2(config-gei_2/1)exit
//connect ZXR10-3
ZXR10_S2(config)#interface gei_2/2
ZXR10_S2(config-gei_2/2)negotiation auto
ZXR10_S2(config-gei_2/2)switchport mode trunk
ZXR10_S2(config-gei_2/2)switchport trunk vlan 100-200
ZXR10_S2(config-gei_2/2)switchport trunk vlan 4000
ZXR10_S2(config-gei_2/2)exit
 //connect ZXR10-4
ZXR10_S2(config)#interface gei_2/3
ZXR10_S2(config-gei_2/3)negotiation auto
ZXR10_S2(config-gei_2/3)switchport mode trunk
ZXR10_S2(config-gei_2/3)switchport trunk vlan 100-200
ZXR10_S2(config-gei_2/3)switchport trunk vlan 4000
ZXR10_S2(config-gei_2/3)exit

ZXR10_S2(config)#zesr ctrl-vlan 4000 protect-instance 1
ZXR10_S2(config)#zesr ctrl-vlan 4000 major level role
zess-master gei_2/2 gei_2/1          //configure zess-master node
/*Note:Secondary interface decides blocking location, therefore ,
therefore Secondary interface can' t be configured on corresponding
 interface of link between ZXR10-2 and ZXR10-3 or blocking interface
 faulty will occur.*/
ZXR10_S2(config)#zesr ctrl-vlan 4000 level 1 seg 1 role
edge- assistant gei_2/3  //configure ordinary ZESR border node role
```

Node 3 configuration:

The configuration such as interface instance of node 3 is the same as that of node 2.

```
//Configure ZESR+ Tansit node
ZXR10_S3(config)#zesr ctrl-vlan 4000 protect-instance 1
ZXR10 s3(config)#zesr ctrl-vlan 4000 major-level role zess-transit
 gei_3/2 gei_3/1        //configure zess-transit node
/*When configuring zess-transit role, note that Primary interface
 decides the direction that node sends hello frame, therefor
Primary interface must be configured the corresponding interface
 of link between ZXR10-2 and ZXR10-3, or configuration error will occur.*/
ZXR10 s3(config)#zesr ctrl-vlan 4000 level 1 seg 1 role edge-assistant
 gei_3/3 //configure ordinary ZESR border node role
```

Node 4 configuration:

The configuration such as interface instance of node 4 is the same as that of node 2.

```
//Configure ZESR low-level main node
ZXR10_S4(config)#zesr ctrl-vlan 4000 protect-instance 1
ZXR10 s4(config)#zesr ctrl-vlan 4000 level 1 seg 1 role master
 gei_4/2 gei_4/1  //configure ordinary ZESR master role
```

This page is intentionally blank.

Chapter 17

Security Configuration

Table of Contents

IP Source Guard

IP Source Guard Overview

IP Source Guard is an application based on DHCP SNOOPING.It records dynamic user information (IP, MAC) by constructing DHCP SNOOPING binding database. After enabling this function, user only can use the address that DHCP server dynamically distributes to access external network. This prevents other users from using other IP address for deceit.

Configuring IP Source Guard

To configure IP Source Guard or delete IP Source Guard, use the following commands.

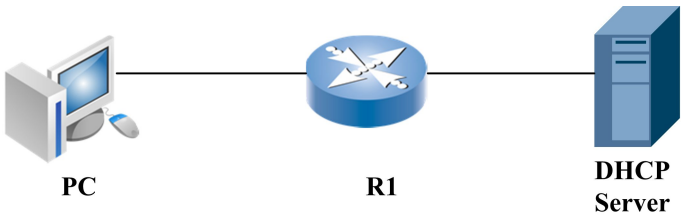
Step	Command	Function
1	ZXR10(config-if-vlanX)#**ip dhcp snooping ip-source-guard** { **ip-base**| **mac-base**| **mac-ip-base** }[**vlan** { **default** |<*vlan-id*>}]	This configures IP Source Guard of interface.
2	ZXR10(config-if-vlanX)#**no ip dhcp snooping ip-source-guard**	This deletes IP Source Guard of interface.

IP Source Guard Configuration Example

IP Source Guard Configuration based on IP Address

In Figure 36, DHCP server connects gei_1/1 on R1, administrator sets management DHCP, gei_1/1 belongs to vlan100. DHCP Snooping function is enabled in VLAN100 and interface gei_1/1 is configured as trusted. PC connects gei_1/2 of switch, which belongs to vlan100.

FIGURE 36 IP SOURCE GUARD CONFIGURATION



IP Source Guard based on IP address is configured on the gei_1/2 interface mode. After getting IP address dynamically, PC can only pass the data packet with source IP address that is distributed by DHCP server.

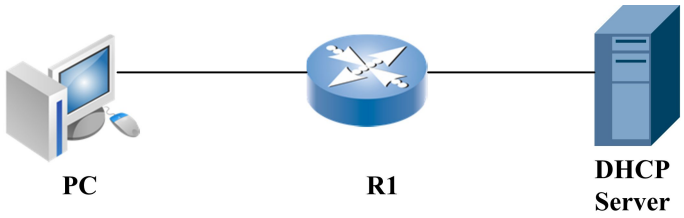
Configuration of R1:

```
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#ip dhcp snooping trust gei_1/1
XR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#ip dhcp snnoping ip-source-guard ip-base
```

IP Source Guard Configuration based on MAC Address

In Figure 37, DHCP server connects gei_1/1 on R1, administrator sets management DHCP, gei_1/1 belongs to vlan100. DHCP Snooping function is enabled in VLAN100 and interface gei_1/1 is configured as trusted. PC connects gei_1/2 of switch, which belongs to vlan100.

FIGURE 37 IP SOURCE GUARD CONFIGURATION



IP Source Guard based on MAC address is configured on the gei_1/2 interface mode. Afer getting IP address dynamically, PC can only pass the data packet with source MAC address that is local host NIC card.

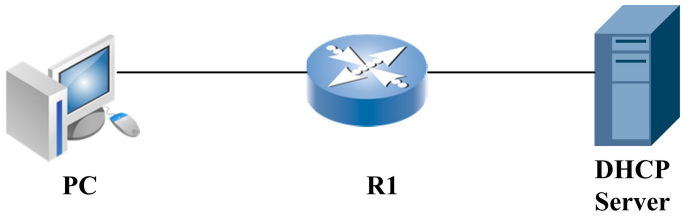
Configuration of R1:

```
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#ip dhcp snooping trust gei_1/1
ZXR10(config)#interface gei_1/2
ZXR10(config-if)#ip dhcp snnoping ip-source-guard mac-base
```

IP Source Guard Configuration based on IP Address and MAC address

In Figure 38, DHCP server connects gei_1/1 on R1, administrator sets management DHCP, gei_1/1 belongs to vlan100. DHCP Snooping function is enabled in VLAN100 and interface gei_1/1 is configured as trusted. PC connects gei_1/2 of switch, which belongs to vlan100.

FIGURE 38 IP SOURCE GUARD CONFIGURATION



IP Source Guard based on MAC address is configured on the gei_1/2 interface mode. After getting IP address dynamically, PC can only pass the data packet with source MAC address that is local host NIC card and source IP address that is distributed by DHCP server.

Configuration of R1:

```
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 100
ZXR10(config)#ip dhcp snooping trust gei_1/1
ZXR10(config)#interface gei_1/2
ZXR10(config-if)#ip dhcp snnoping ip-source-guard mac-ip-base
```

Control Plane Security Configuration

Control Plane Security Overview

Internet and IP technology wildspread application bring the great change to the world. With IP network being developed widely and deeply, network attack and virus are becoming more and more frequent, which brings people much visible and invisible loss. The previous network attack and virus mostly take PC or server host as major attack objects. But now terminal end user anti-virus capability and virus maker capability increases day by day, the network devices such as router and switch become the object that virus attacks.

According to known or predictable attack and virus on the switch, we can take many kinds of measures to make switch have self-protection and safeguarding network security capability. The main function of control plane security is to monitor the packet uploading rate, generate alarm on abnormal rate uploading packet and remind network manager to pay attention to possible packet attack to CPU. So that network manager can decide if discard this packet on the interface or limit speed and filter unreasonable packet.

Command Configuration

1. To enable/disable control-plane-security function, use the following command.

Command	Function
ZXR10(config)#**control-plane-security** {**enable** | **disable**}	This command is control-plane-security function global switch. It is used to open or close control-plane-security function, the default is enabled.

2. To discard or pass protocol packet, use the following command.

Command	Function
ZXR10(config-gei_1/x)#**protocol-protect mode** <*protocolname*>{**enable** | **disable**}	This passes/discards protocol packet.

This command is configured in the interface mode. Configuration decides if a certain protocol packet will be discarded in a physical port. As for the port whose port configuration is NNI, all configured protocol packets are enabled in default. But as for the port whose port configuration is UNI, the default value

is different according to different protocol packets, which can be viewed by show command.

3. To configure protocol packet alarm threshold, use the following command.

Command	Function
ZXR10(config-gei_1/x)#**protocol-protect alarm mode** <*protocol name*>< *alarm-limit* >	This configures a certain protocol packet alarm threshold as 30s. The alarm-limit range is 1000-18000.

This command is also configured in the interface mode. It is used to modify a certain protocol packet alarm threshold in a certain physical port. When the number of specific protocol packet exceeds this threshold in 30s, an alarm message is sent to user. The default value is 3000.

4. To configure protocol packet passing peak/average speed, use the following command.

Command	Function
ZXR10(config-gei_1/x)#**protocol-protect** {**peak-rate** | **average-rate**} **mode** <*protocol name*>< *rate-limit* >	This configures protocol packet passing peak/average speed.

This command is used to configure peak speed or average speed of corresponding protocol packet on corresponding port. The unit is pps, peak speed can be configured 100~1000 and the default value is 300, average speed can be set 10~600 and the default is 100.

5. To configure port type, use the following command.

Command	Function
ZXR10(config-gei_1/x)#**protocol-protect type** {**nni** | **uni**}	This configures the type of a certain port is uni or nni.

This command is used to configure a certain port type which is uni or nni. The default is nni.

The above commands supporting protocol includes: pim igmp icmp arpreply arprequest udld, group mng vbase lldp, dhcp lacp bpdu snmp, na ns ra rs.

When protocol packet is configured discard, even if uploaded to MUX module, it will be discarded by this module, which leads to fail to upload to platform. When control-plane-security module find that the speed of a certain protocol packet uploading to platform is too fast, it will send alarm to remind user that maybe there is a certain protocol packet to attack CPU. When seeing this alarm, user can configure protocol packet discard or limit speed to prevent attack from CPU.

Note:

The discard of some protocol packets will make the corresponding service invalid.

Configuration Example

1. This example shows how to configure port arp protocol and set alarm threshold as 2500.

```
Zxr10#conf t
Zxr10(config)#inter gei_1/1
Zxr10(config-gei_1/1)# protocol-protect mode arp enable
Zxr10(config-gei_1/1)# protocol-protocol alarm mode arp 2500
```

2. This example shows how to configure icmp protocol packet passing peak/average speed.

```
Zxr10#conf t
Zxr10(config)#inter gei_1/1
Zxr10(config-gei_1/1)# protocol-protect peak-rate mode icmp 500
Zxr10(config-gei_1/1)# protocol-protocol average-mode mode icmp 250
```

Maintenance and Diagnosis

ZXR10 5900/5200 provides **show** command to help maintenance and diagnosis. Common commands used in control-plane-security maintenance and diagnosis are as follows.

Step	Command	Function
1	ZXR10(config)#**show protocol-protect packet-config** <*interfacename*>	This views a certain port type and the protocol packet configuration and receiving statistics on this port.
2	ZXR10(config)#**show protocol-protect token-buckets** <*interfacename*>	This views protocol packet receiving speed configuration and statistics on a certain port.
3	ZXR10#**clear protocol-protect** {**packets-count** | **buckets-count**}<*interfacename*>	This clears protocol statistic count on a certain port.

DAI Configuration

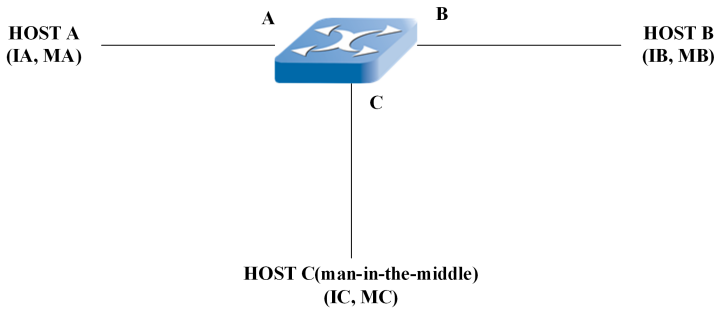
DAI Overview

The attack based on ARP often happens in network. DHCP SNOOPING module on the switch implements DAI (Dynamic ARP Inspection) function, but this function is limited.

Currently DAI function only checks binding table in DHCP SNOOPING for switch learning ARP packet, that is, only can check layer 3 user.

If users of the switch are in the same VLAN, the communication between users requires switch to forward not on layer 3 but layer 2. Switch need not to learn ARP packets of these users. Therefore there isn't relevant security check. It is a big security bug, which causes man-in-the-middle attack, as shown in Figure 39.

FIGURE 39 MAN-IN-THE-MIDDLE ATTACK



A/B/C are in the same broadcast domain, that is, the same network segment. When A and B communicates with each other, ARP packet is sent first, which can be learned by C. If C acts as man-in-the-middle to do malicious scanning, only sends free ARP to A to inform that IP corresponding MAC address of B has been updated to that of C, the flow from A to B is directly forwarded to C; Based on the same principle the flow from B to A can be forwarded to C. After doing malicious scanning on packet, C modifies the destination address as the real MAC address of B or A and return the packet to switch. The flow between A and B can be forwarded normally and not be perceived. So that C completes man-in-the-middle attack.

To avoid this bug, all ARP packets should be checked. Those that conform to the qualification are forwared by software. The ARP packets that fail in check will be discarded.

Based on this requirement, the following methods that prevents usual ARP attack are added.

1. As for untrusted interface, DAI blocks all ARP packets and send them to upper layer software for check.
2. The speed that ARP packet sent to CPU is configurable.
3. When DHCP SNOOPING is enabled, laye 2 IP ,MAC and port corresponding relationship are checked. Illegal user will be discarded.

DAI detects ARP packet according to the binding relationship between IP and MAC address which is stored in trust database. When DHCP SNOOPING of VLAN is open, database is created by DHCP SNOOPING. If ARP packet is received from a trust port, switch need not any detection and forwards packet directly. If ARP packet is received from a untrust port, switch only forwards valid packet.

Configuring DAI

Step	Command	Function
1	`Zxr10(config-gei_1/x)#`**ip arp inspection trust**	This configures trust attribute of interface.
2	`Zxr10 (config-smartgroupX)#`**ip arp inspection trust**	This configures trust attribute of Smartgroup interface.
3	`Zxr10(config)#`**ip arp inspection validate** {[**des-mac**][**ip**][**src-mac**]}	This configures global ARP validate inspection function.
4	`Zxr10 (config-gei_1/x)#`**ip arp inspection limit** *<1-100>*	This configures the limited speed of interface. As for untrusted interface, the default is 15pps. As for trusted interface, ARP packet speed is not limited.
5	`Zxr10(config-vlanX)#`**ip arp inspection**	This configures DAI enabled of VLAN.

DAI Maintenance and Diagnosis

ZXR10 5900/5200 provides **show** command to help maintenance and diagnosis. Common commands used in DAI maintenance and diagnosis are as follows.

1. To view trusted attribute of interface, use the following command.

   show ip arp inspection {**interface interface_name**}

2. To view ARP packet validated inspection information, use the following command.

   show ip arp inspection configure

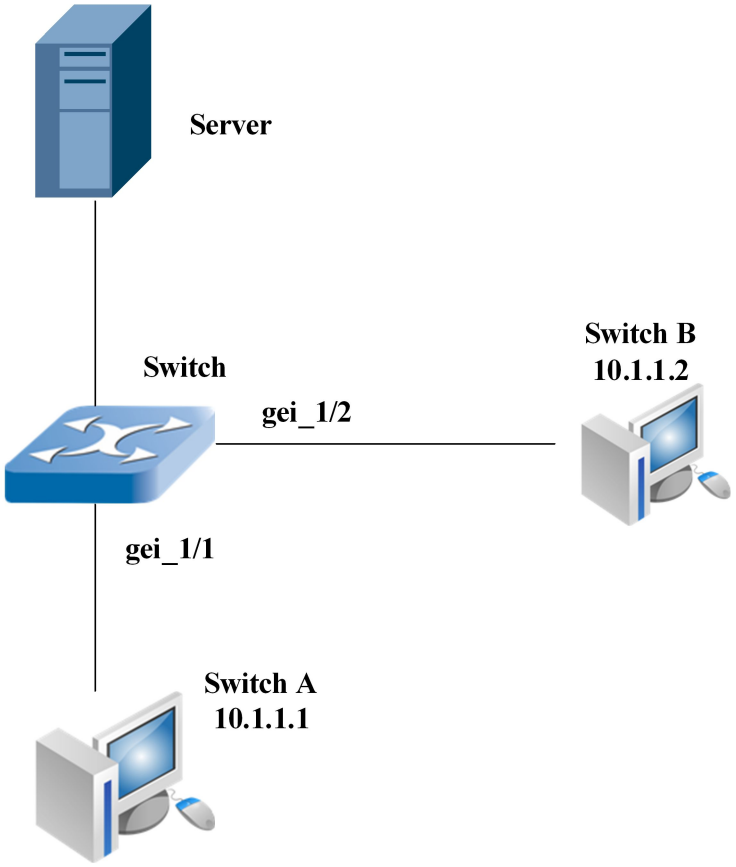
3. To view DAI configuration information of VLAN, use the following command.

   show ip arp inspection vlan [{*<1-4094>*| **disable** | **enable** | **name vlan_name**}]

DAI Configuration Example

As shown in Figure 40, VLAN 2 is configured on switch and DAI is run.

FIGURE 40 DAI CONFIGURATION EXAMPLE



Prerequisites: DHCP SNOOPING function is opened in VLAN 2.

```
ZXR10(config)#ip dhcp snooping enable
ZXR10(config)#ip dhcp snooping vlan 2
```

VLAN 2 is configured on switch A and DAI is run.

```
ZXR10(config-vlan2)#ip arp inspection
```

Gei_1/1 and gei_1/2 are bound with VLAN 2.

Gei_1/1 is set as untrusted interface (the default attribute is untrusted interface).

The legal ARP packet(legal ARP packet: consistent witch IP+ port+ MAC in DHCP binding table) that host A sends to switch is broadcast in VLAN. Host B can receive ARP packet. The illegal packet is discarded and not forwarded. Host B can't receive ARP packet.

If gei_1/1 is set as trusted interface,

host A sends ARP packet(legal/illegal) to switch. Switch forwards ARP packet by hardware to all interfaces that are bound with VLAN 1. Host B can receive ARP packet. When configuring interface lim-

ited speed as X(1-100), switch will receive at most X ARP packets every second, the additional are discarded.

MFF Configuration

MFF Overview

MFF MAC-Forced Forwarding mainly implements layer 2 isolation and layer 3 intercommunication among different client hosts in the same broadcast domain. MFF blocks user ARP request packet and reply response packet of gateway MAC address by ARP answer-agent mechanism. This way can force user to send all traffic (includes traffic in the same subnet) to gateway, which makes gateway monitor data flow, prevent malicious attack among users and ensure safety of network deployment.

MFF supports manual and automatic modes. Manual mode is applied in user static IP address configuration scene. Automatic mode is used in user dynamically getting IP address by DHCP protocol scene.

Configuring MFF

1. To set MFF mode, use the following commands.

Step	Command	Function
1	`ZXR10(config)#`**mff mode** {**auto** | **manus**}	This configures MFF manual mode or automatic modes.
2	`ZXR10(config)#`**no mff mode**	This cancels MFF mode configuration.

2. To enable MFF function, use the following command.

Step	Command	Function
1	`ZXR10(config-if-vlanX)#`**mff enable**	This enables MFF function in VLAN interface.
2	`ZXR10(config-if-vlanX)#`**no mff mode**	This disables MFF function in VLAN interface.

3. To configure MFF interface type, use the following command.

Step	Command	Function
1	ZXR10(config-gei_1/x)#**set mff** {**user-port** | **network-port**}	This sets layer 2 physical interface as MFF user interface or network interface.
2	ZXR10(config-gei_1/x)#**no set mff**	This cancels MFF interface type.

4. To configure MFF gateway IP address, use the following command.

Step	Command	Function
1	ZXR10(config-if-vlanX)#**set mff gateway ip** *<A.B.C.D>*	This configures MFF gateway IP address in VLAN by manual mode.
2	ZXR10(config-if-vlanX)#**no set mff gateway ip**	This cancels MFF gateway IP address.

5. To configure MFF user statically, use the following command.

Step	Command	Function
1	ZXR10(config)#**mff user** *<A.B.C.D><H.H.H>* **vlan** *<1-4094>* **gateway** *< A.B.C.D >*	This configures MFF user statically in manual mode.
2	ZXR10(config)#**no mff user** *<A.B.C.D>* **vlan** *<1-4094>*	This clears statically configured MFF user.

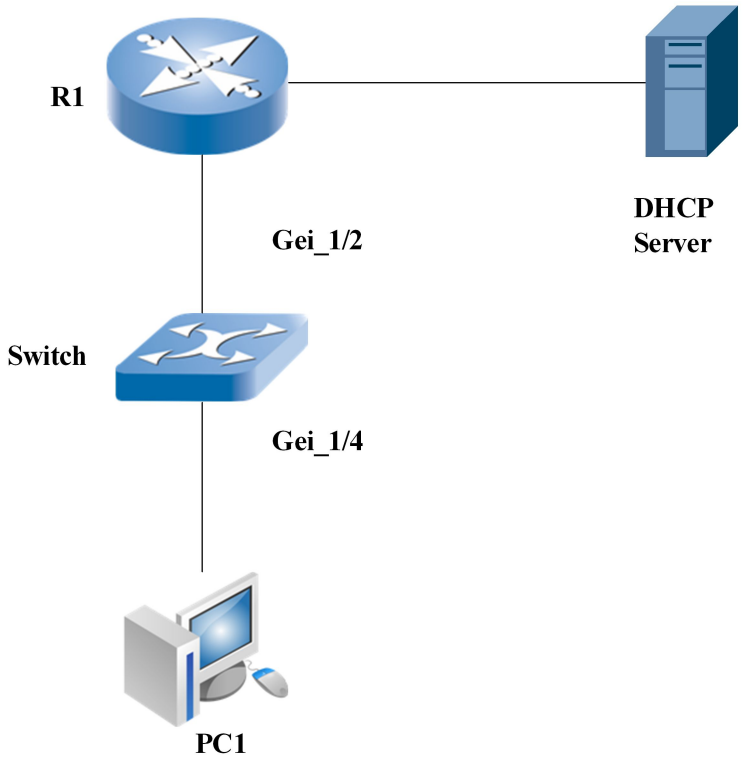
6. To enable MFF gateway MAC address detection function, use the following commands.

Step	Command	Function
1	ZXR10(config)#**mff gateway detect enable**	This enables MFF gateway MAC address detection function.
2	ZXR10(config)#**mff gateway detect disable**	This disables MFF gateway MAC address detection function.

MFF Configuration Example

As shown in Figure 41, R1 is MFF gateway. PC1 obtains IP address through DHCP. DHCP SNOOPING and MFF are configured on switch

FIGURE 41 MANUAL MODE BASIC MFF FUNCTION CONFIGURATION EXAMPLE



MFF configuration of switch:

```
ZXR10(config)#mff mode auto
ZXR10(config)#mff gateway detect enable
ZXR10(config)#interface vlan 1
ZXR10(config-if-vlan1)#ip address 192.168.1.100 255.255.255.0
ZXR10(config-if-vlan1)#mff enable
ZXR10(config-if-vlan1)#exit
ZXR10(config)#interface gei_1/2
ZXR10(config-gei_1/2)#set mff network-port
ZXR10(config-gei_1/2)#exit
ZXR10(config)#interface gei_1/4
ZXR10(config-gei_1/4)#set mff user-port
```

MFF maintenance and diagnosis

When MFF encounters problem, we can locate the fault and remove them with relevant debugging commands. The mostly used command is show command.

1. This displays MFF global configuration information.

   show mff configure

   Example: This configures global configuration information manually.

   ```
   ZXR10# show mff configure
    MFF Mode :manus
   MFF Gateway MAC detecting  :disable
   ```

2. This displays MFF VLAN configuration information.

   show mff vlan <*vlan-id*>

   Example: This designates VLAN configuration information manually.

```
ZXR10#show mff vlan 1
MFF function: enable
MFF gateway ip: 10.40.20.1
```

3. This displays MFF physical interface configuration information.

   show mff interface [<*interface-name*>]

   The command with interface name will view configuration information of designated interface; The command without parameter will view all opened MFF function configuration information.

   Example: view configuration information of the designated interface.

```
ZXR10#show mff interface gei_1/1
Interface      MFF Type
-------------   -------------
gei_1/1         Network port
```

4. This views MFF corresponding relationship table.

   show mff-table [**vlan** <*vlan-id*>[**A.B.C.D**]]

   Command Illustration:

   i. The command without option will view all MFF corresponding relationship.

   ii. The command with VLAN option will view all MFF corresponding relationship in this VLAN.

   iii. The command with VLAN and user IP address option will view MFF corresponding relationship of specific user.

   iv. Illustration to displayed command information:

Information	**Description**
IP Address	Subscriber's IP address
Type	Entry Type
Hardware Address	User MAC Address
VlanID :	User VLAN ID

This page is intentionally blank.

Chapter 18

POE Configuration

Table of Contents

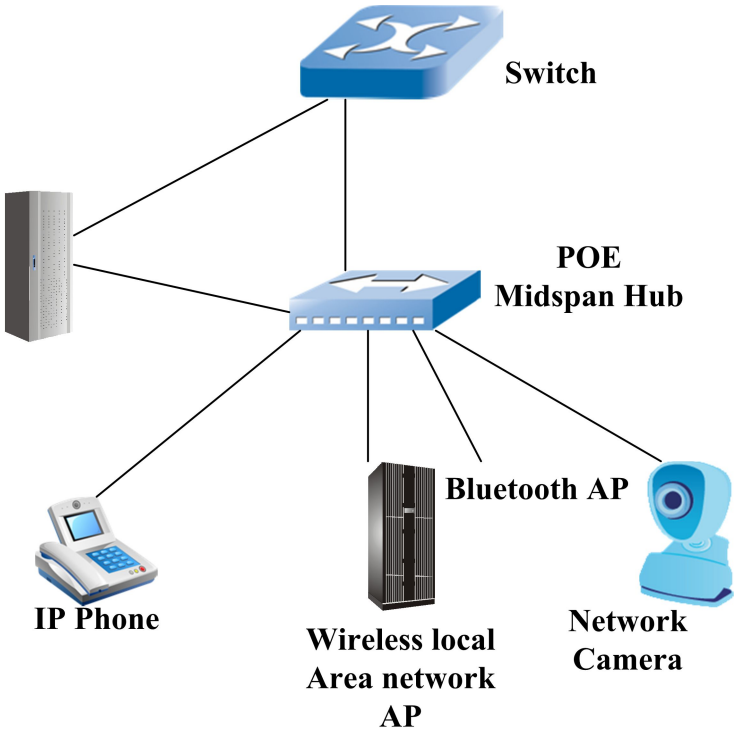
POE Overview

PoE Power over Ethernet is an extended feature of network device that supports Ethernet electrical interface. The network device supporting PoE function such as switch and router can provide power supply to remote PD including IP phone, WLANE AP and Network Camera through twisted pair for implementing remote power supply.

Ethernet remote power supply sometimes is called network power supply. It is the technology that transfers power through 10 BaseT and 100 Base-TX. When the current Ethernet Cat.5 infrastructure doesn't change, data signal can be transmitted to the terminals based on IP (such as IP phone, AP and network camera and DC power can be supplied to those at the same time. PoE technology can ensure the structured cabling security and the current network normal operation to decrease the cost greatly.

Figure 42 displays a common PoE power supply example.

FIGURE 42 POE POWER SUPPLY



Configuring PoE

Step	Command	Function
1	ZXR10 (config-if) #**poe enable**	This enables interface PoE function. The default is disabled.
2	ZXR10 (config-if) #**poe pd-max-power** [**15.4** | **7.0** | **4.0** | **ext.18**| **ext.27**|**ext.30.0**]	This configures port maximum power. This command only can be used when this interface doesn't be enabled PoE function. The default is 15.4.
3	ZXR10 (config-if) #**poe priority** [**critical** | **high** | **low**]	This configures interface priority. This command only can be used when this interface doesn't be enabled PoE function. The default is low.

Step	Command	Function
4	ZXR10 (config-if) #**poe enhanced-mode** [**enable** | **disable**]	This configures compatibility detection of port connected device. This command only can be used when this interface doesn't be enabled PoE function. The default is enabled. This command indicates whether to open the connected device compatibility detection. If enable is configured, power will be supplied on port when non-standard PD device (cisco big capacity device) is detected. If disable is configured, power will be supplied only when standard PD device is detected.
5	ZXR10 (config) #**poe overtemperature auto-recovery enable**	This configures switch temperature recovery. When device works at stack mode, the command format is **poe overtemperature auto-recovery enable device-id** <*device-id*> The default is disabled.
6	ZXR10 (config#**poe power-threshold** <*40-90*>	This configures switch power occupancy alarm threshold. When device works in stack mode, this command format is **poe power-threshold** <*40-90*> **device-id** <*device-id*>. The default is 80.
7	ZXR10 (config) #**poe upgrade-firmware** {**firmware-name**}	This upgrades firmware used in device. When device works in stack mode, this command format is **poe upgrade-firmware** {**firmware-name**} **device-id** <*device-id*>. This command upgrades Firmware PSE handling software on-line.

PoE Configuration Example

This examples shows the PoE configuration on switch in a stack system.

```
ZXR10(config)#int gei_2/1/5
ZXR10(config-gei_2/1/5)#poe priority high
```

```
ZXR10(config-gei_2/1/5)#poe pd-max-power ext.27
ZXR10(config-gei_2/1/5)#poe enhanced-mode enable
ZXR10(config-gei_2/1/5)#poe enable
ZXR10(config-gei_2/1/5)#exit
ZXR10(config)#poe overtemperature auto-recovery enable device-id 2
ZXR10(config)#poe power-threshold 88 device-id 2
```

PoE Maintenance

ZXR10 5900/5200 provides **show** command to help maintenance and diagnosis of PoE. Common commands used in PoE maintenance and diagnosis are as follows.

Step	Command	Function
1	ZXR10(config)#**show poe config interface** <*infterface-name*>	This views interface PoE configuration.
2	ZXR10(config)#**show poe interface** <*infterface-name*>	This views interface PoE status configuration.
3	ZXR10(config)#**show poe device** <*device-id*>	This views PSE status information.

Figures

Tables

This page is intentionally blank.

Glossary

DHCP - Dynamic Host Configuration Protocol
BRAS - Broadband Remote Access Server
DWRR - Deficit Weighted Round Robin
CLI - Command Line Interface
CIR - Committed Information Rate
DSCP - Differentiated Services Code Point
CBS - Committed Burst Size
EAPOL - Extensible Authentication Protocol Over LAN
IP - Internet Protocol
MAC - Media Access Control
LLDPDU - Link Layer Discovery Protocol Data Unit
IPTV - Internet Protocol Television
FTP - File Transfer Protocol
LLDP - Link Layer Discovery Protocol
ICMP - Internet Control Message ProtocolInternet
MIB - Management Information Base
NTP - Network Time Protocol
EBS - Excess Burst Size
SP - Strict Priority
SNMP - Simple Network Management Protocol
PVID - Port VLAN ID
SSH - Secure Shell
PIR - Peak Information Rate
PBS - Peak Burst Size
RADIUS - Remote Authentication Dial In User Service
RMON - Remote Monitoring
QoS - Quality of Service
STP - Spanning Tree Protocol
TELNET - Telecommunication Network Protocol
TFTP - Trivial File Transfer Protocol
UDP - User Datagram Protocol
URPF - Unicast Reverse Path Forwarding
UDLD - UniDirectional Link Detection
TTL - Time To Live
ToS - Type Of Service

TCP - Transmission Control Protocol

TLV - Type Length Value

VBAS - Virtual Broadband Access Server

VLAN - Virtual Local Area Network

WRR - Weighted Round Robin

ACL - Access Control List

BAS - Broadband Access Server

AAA - Authentication, Authorization, and Accounting

ARP - Address ResolutionProtocol

CoS - Class of Service

DSLAM - Digital Subscriber Line Access Multiplexer